Alcatel·Lucent

Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R7

USER GUIDE

3HE 06495 AAAG TQZZA Edition 01

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

When printed by Alcatel-Lucent, this document is printed on recycled paper.

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

1.1 Subject to the terms and conditions of this Agreement, Alcatel-Lucent grants to Customer and Customer accepts a nonexclusive, nontransferable license to use any software and related documentation provided by Alcatel-Lucent pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel-Lucent. In case of equipment failure, Customer may use the Licensed Program on a backup system, but only for such limited time as is required to rectify the failure.

1.2 Customer acknowledges that Alcatel-Lucent may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate workstations, paths and partitions), which may be increased upon the purchase of the applicable license extensions.

1.3 Use of the Licensed Program may be subject to the issuance of an application key, which shall be conveyed to the Customer in the form of a Supplement to this End User License Agreement. The purchase of a license extension may require the issuance of a new application key.

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

2.1 Customer acknowledges and agrees that the Licensed Program contains proprietary and confidential information of Alcatel-Lucent and its third party suppliers, and agrees to keep such information confidential. Customer shall not disclose the Licensed Program except to its employees having a need to know, and only after they have been advised of its confidential and proprietary nature and have agreed to protect same.

2.2 All rights, title and interest in and to the Licensed Program, other than those expressly granted to Customer herein, shall remain vested in Alcatel-Lucent or its third party suppliers. Customer shall not, and shall prevent others from copying, translating, modifying, creating derivative works, reverse engineering, decompiling, encumbering or otherwise using the Licensed Program except as specifically authorized under this Agreement. Notwithstanding the foregoing, Customer is authorized to make one copy for its archival purposes only. All appropriate copyright and other proprietary notices and legends shall be placed on all Licensed Programs supplied by Alcatel-Lucent, and Customer shall maintain and reproduce such notices on any full or partial copies made by it.

3. TERM

3.1 This Agreement shall become effective for each Licensed Program upon delivery of the Licensed Program to Customer.

3.2 Alcatel-Lucent may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel-Lucent is not paid within thirty (30) days of the date on which payment is due; (b) if Customer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator; (c) if bankruptcy, reorganization or insolvency proceedings are instituted against Customer and not dismissed within 15 days; or (d) if Customer breaches a material provision of this Agreement and such breach is not rectified within 15 days of receipt of notice of the breach from Alcatel-Lucent.

3.3 Upon termination of this Agreement, Customer shall return or destroy all copies of the Licensed Program. All obligations of Customer arising prior to termination, and those obligations relating to confidentiality and nonuse, shall survive termination.

4. CHARGES

4.1 Upon shipment of the Licensed Program, Alcatel-Lucent will invoice Customer for all fees, and any taxes, duties and other charges. Customer will be invoiced for any license extensions upon delivery of the new software application key or, if a new application key is not required, upon delivery of the extension. All amounts shall be due and payable within thirty (30) days of receipt of invoice, and interest will be charged on any overdue amounts at the rate of 1 1/2% per month (19.6% per annum).

5. SUPPORT AND UPGRADES

5.1 Customer shall receive software support and upgrades for the Licensed Program only to the extent provided for in the applicable Alcatel-Lucent software support policy in effect from time to time, and upon payment of any applicable fees. Unless expressly excluded, this Agreement shall be deemed to apply to all updates, upgrades, revisions, enhancements and other software which may be supplied by Alcatel-Lucent to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

6.1 Alcatel-Lucent warrants that the Licensed Program as originally delivered to Customer will function substantially in accordance with the functional description set out in the associated user documentation for a period of 90 days from the date of shipment, when used in accordance with the user documentation. Alcatel-Lucent's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel-Lucent's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel-Lucent is unable to rectify the nonconformity, Alcatel-Lucent shall accept return of the Licensed Program and shall refund to Customer all amounts paid in respect thereof. This warranty is available only once in respect of each Licensed Program, and is not renewed by the payment of an extension charge or upgrade fee.

6.2 ALCATEL-LUCENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, REPRESENTATIONS, COVENANTS OR CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED PROGRAM WILL BE ERROR FREE OR THAT THE LICENSED PROGRAMS WILL NOT INFRINGE UPON ANY THIRD PARTY RIGHTS.

6.3 Alcatel-Lucent shall defend and indemnify Customer in any action to the extent that it is based on a claim that the Licensed Program furnished by Alcatel-Lucent infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel-Lucent within ten (10) days of the existence of the claim, gives Alcatel-Lucent sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel-Lucent may reasonably require. Notwithstanding the foregoing, Alcatel-Lucent shall have no liability if the claim results from any modification or unauthorized use of the Licensed Program by Customer, and Customer shall defend and indemnify Alcatel-Lucent against any such claim.

6.4 Alcatel-Lucent Products are intended for standard commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The Customer hereby agrees that the use, sale, license or other distribution of the Products for any such application without the prior written consent of Alcatel-Lucent, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the Products in such applications.

7. LIMITATION OF LIABILITY

7.1 IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE LICENSED PROGRAM THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL-LUCENT HEREUNDER. NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.2 The foregoing provision limiting the liability of Alcatel-Lucent's employees, agents, officers and directors shall be deemed to be a trust provision, and shall be enforceable by such employees, agents, officers and directors as trust beneficiaries.

8. GENERAL

8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.

8.2 This Agreement constitutes the entire agreement between Alcatel-Lucent and Customer and supersedes all prior oral and written communications. All amendments shall be in writing and signed by authorized representatives of both parties.

8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be severed and the remaining provisions shall continue in full force and effect.

8.4 The Licensed Program may contain freeware or shareware obtained by Alcatel-Lucent from a third party source. No license fee has been paid by Alcatel-Lucent for the inclusion of any such freeware or shareware, and no license fee is charged to Customer for its use. The Customer agrees to be bound by any license agreement for such freeware or shareware. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE PROVIDES NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF CUSTOMER'S POSSESSION AND/OR USE OF THE FREEWARE OR SHAREWARE.

8.5 Alcatel-Lucent shall have the right, at its own expense and upon reasonable written notice to Customer, to periodically inspect Customer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Customer's compliance with its obligations under this Agreement.

8.6 All notices shall be sent to the parties at the addresses listed above, or to any such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.

8.7 If the Licensed Program is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Program is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only "restricted rights" in the Licensed Program as defined in DFARS 227-7202-1(a) and 227.7202-3(a), or equivalent. If the Licensed Program is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 52.227-19 or 52.227-14 of the FAR, or if acquired by NASA, Clause 18-52.227-86(d) of the NASA Supplement to the FAR, or equivalent. If the software was acquired under a contract subject to the October 1988 Rights in Technical Data and Computer Software regulations, use, duplication and disclosure by the Government is subject to the restrictions set forth in DFARS 252-227.7013(c)(1)(ii) 1988, or equivalent.

8.8 Customer shall comply with all export regulations pertaining to the Licensed Program in effect from time to time. Without limiting the generality of the foregoing, Customer expressly warrants that it will not directly or indirectly export, reexport, or transship the Licensed Program in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of any right hereunder, or of the failure to perform or of a breach by the other party, shall not be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.

8.10 This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite, including this guide.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM customer documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
5620 SAM Release Description	The *5620 SAM Release Description* provides information about the new features associated with a 5620 SAM software release.

(1 of 4)

Guide	Description
5620 SAM Planning Guide	The *5620 SAM Planning Guide* provides information about 5620 SAM scalability and recommended hardware configurations.
5620 SAM System Architecture Guide	The *5620 SAM System Architecture Guide* is intended for technology officers and network planners to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
5620 SAM | 5650 CPAM Installation and Upgrade Guide	The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to a different system • conversion from a standalone to a redundant 5620 SAM system
5620 SAM User Guide	The *5620 SAM User Guide* provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, commissioning, service configuration, and policy management. The *5620 SAM User Guide* uses a task-based format. Each chapter contains: • a workflow that describes the steps for configuring and using the functions • detailed procedures that list the configurable parameters on the associated forms 5620 SAM management information specific to LTE network elements is covered in the *5620 SAM LTE ePC User Guide* and *5620 SAM LTE RAN User Guide*. 5620 SAM management information specific to 1830 PSS network elements is covered in the *5620 SAM Optical User Guide*.
5620 SAM Integration Guide	The *5620 SAM Integration Guide* provides procedures to allow the 5620 SAM to integrate with additional components.
5620 SAM Supervision Module User Guide	The *5620 SAM Supervision Module User Guide* provides information about how to configure and use the web-based 5620 SAM Supervision Module for fault management and at-a-glance network element monitoring.
5620 SAM Scripts and Templates Developer Guide	The *5620 SAM Scripts and Templates Developer Guide* provides information that allows you to develop, manage, and execute CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: • CLI scripting, XML, and the Velocity engine • basic scripting or programming • 5620 SAM functions
5620 SAM Parameter Guide	The *5620 SAM Parameter Guide* provides: • parameter descriptions that include value ranges and default values • parameter options and option descriptions • parameter and option dependencies • parameter mappings to the 5620 SAM-O XML equivalent property names There are dynamic links between the procedures in the *5620 SAM User Guide* and the parameter descriptions in the *5620 SAM Parameter Guide*. Parameters specific to LTE network elements are covered in the *5620 SAM LTE Parameter Reference*. Parameters specific to 1830 PSS network elements are covered in the *5620 SAM Optical Parameter Reference*.
5620 SAM Statistics Management Guide	The *5620 SAM Statistics Management Guide* provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.

(2 of 4)

Guide	Description
5620 SAM Maintenance Guide	The *5620 SAM Maintenance Guide* provides procedures for: • generating baseline information for 5620 SAM applications • performing daily, weekly, monthly, and as-required maintenance activities for 5620 SAM-managed networks

5620 SAM Troubleshooting Guide	The *5620 SAM Troubleshooting Guide* provides task-based procedures and user documentation to:
	• help resolve issues in the managed and management networks
	• identify the root cause and plan corrective action for:
	  • alarm conditions on a network object or customer service
	  • problems on customer services with no associated alarms
	• list problem scenarios, possible solutions, and tools to help check:
	  • network management LANs
	  • network management platforms and operating systems
	  • 5620 SAM client GUIs and client OSS applications
	  • 5620 SAM servers
	  • 5620 SAM databases

5620 SAM Alarm Reference	The *5620 SAM Alarm Reference* provides a list of all alarms that the 5620 SAM can raise. The reference is organized by network element type.
5620 SAM Glossary	The *5620 SAM Glossary* defines terms and acronyms used in all of the 5620 SAM documentation, including 5620 SAM LTE documentation.
5620 SAM Network Element Compatibility Guide	The *5620 SAM Network Element Compatibility Guide* provides release-specific information about the compatibility of managed device features in 5620 SAM releases.
5620 SAM LTE documentation	
5620 SAM LTE RAN Release Description	The *5620 SAM LTE RAN Release Description* provides information about the LTE RAN features associated with the release.
5620 SAM LTE ePC User Guide	The *5620 SAM LTE ePC User Guide* describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE ePC User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE RAN User Guide	The *5620 SAM LTE RAN User Guide* describes how to discover, configure, and manage the Evolved NodeB, or eNodeB, using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE RAN User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE Parameter Reference	The *5620 SAM LTE Parameter Reference* provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
5620 SAM-O documentation	
5620 SAM XML OSS Interface Developer Guide	The *5620 SAM XML OSS Interface Developer Guide* provides information that allows you to: • use the 5620 SAM XML OSS interface to access network management information • learn about the information model associated with the managed network • develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
5620 SAM 3GPP OSS Interface Developer Guide	The *5620 SAM 3GPP OSS Interface Developer Guide* describes the components and architecture of the 3GPP OSS interface to the 5620 SAM. It includes procedures and samples to assist OSS application developers to use the 3GPP interface to manage LTE devices.

(3 of 4)

Guide	Description
5620 SAM 3GPP OSS Interface Compliance Statements	The *5620 SAM 3GPP OSS Interface Compliance Statements* document describes the compliance of the 5620 SAM 3GPP OSS interface with the 3GPP standard.
5620 SAM optical documentation	
5620 SAM Optical User Guide	The *5620 SAM Optical User Guide* describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM Optical User Guide* before you attempt to use the 5620 SAM in your network.
5620 SAM Optical Parameter Reference	The *5620 SAM Optical Parameter Reference* provides a list of all optical device parameters supported in the 5620 SAM.
5650 CPAM documentation	
5650 CPAM User Guide	The *5650 CPAM User Guide* describes how to capture, inspect, visualize, and troubleshoot IGP and BGP topologies using the 5650 CPAM.
7701 CPAA Hardware Revision 1 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 1, the route analyzer component of the 5650 CPAM.
7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 2, the route analyzer component of the 5650 CPAM.

(4 of 4)

Obtaining customer documentation

You can obtain 5620 SAM customer documentation:

- from the product
- on the web

On-product documentation

The 5620 SAM on-product customer documentation is delivered in HTML and PDF. Choose Help→User Documentation from the 5620 SAM client GUI to open the help system in a web browser.

The help system opens to the User Documentation Index, which provides a summary of and links to all 5620 SAM customer documents.

Click on the Using the help system tab on the User Documentation Index page to find usage tips for navigating and searching within the on-product customer documentation.

You can return to the User Documentation Index at any time by clicking on the Home icon, shown in Figure 1.

Figure 1 Home icon

Documentation on the web

The 5620 SAM customer documentation is available for download in PDF format from the Alcatel-Lucent Customer Support Center: http://www.alcatel-lucent.com/myaccess. If you are a new user and require access to this service, please contact your Alcatel-Lucent support representative.

In addition to the guides listed in Table 1, Release Notices and other documents not delivered on-product are posted to this site.

Working with PDFs

You can download PDFs of individual guides from the Alcatel-Lucent Customer Support Center, or you can choose to download a zip of all PDFs for a particular release.

You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of any 5620 SAM document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once, provided that they are located in the same directory. For more information, see the Help for Acrobat Reader.

Cross-book hotlinks, for example, from a parameter name in the *5620 SAM User Guide* to a description of that parameter in the *5620 SAM Parameter Guide*, work only if both PDF files are in the same directory.

Note — Users of Mozilla browsers may receive an error message when opening the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the Mozilla Firefox offline storage or Mozilla 1.7 cache value to 100 Mbytes to eliminate the error message.

Documentation conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	*hostname*
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key-Key	Type the appropriate simultaneous keystroke sequence	CTRL-G
*	An asterisk is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵

(1 of 2)

Convention	Description	Example
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

(2 of 2)

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1 This step offers two options. You must choose one of the following.

a This is one option.

b This is another option.

2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.

i This is the first substep.

ii This is the second substep.

iii This is the third substep.

2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the Système international d'unités (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.

Note — Notes provide information that is, or may be, of special interest.

Contents

5620 SAM system management

Device management

12 — Device support 12-1

14 — Device discovery 14-1

15 — Device CLI sessions 15-1

18 — Logical group object configuration 18-1

19 — Shelf object configuration 19-1

Network management

30 — NE routing and forwarding 30-1

31 — Protocol configuration 31-1

32 — MPLS 32-1

33 — Service tunnels 33-1

47 — QoS policies 47-1

62 — NAT policies 62-1

63 — Format and range policies 63-1

Service management

64 — Service management and QoS 64-1

Appendices

Introduction

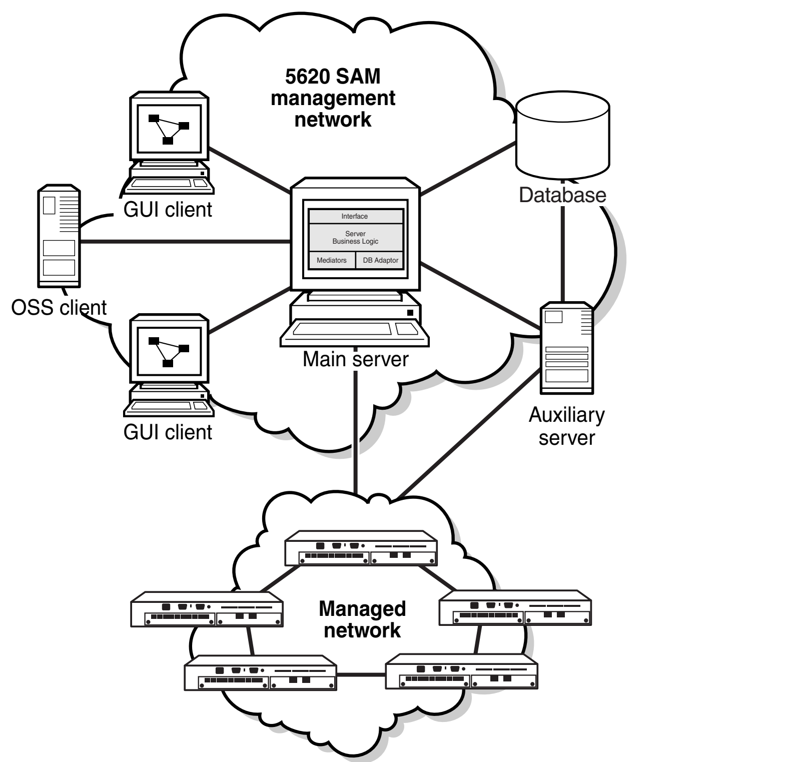
1 — 5620 SAM system overview

1.1 5620 SAM system overview

The 5620 SAM is a system that is designed to manage Alcatel-Lucent network elements, or NEs, such as routers and switches. The 5620 SAM also supports the management of some Telco devices, and provides limited management of other third-party devices, which are called generic NEs.

A 5620 SAM system has client, server, and database components that are deployed in a standalone or redundant configuration. Figure 1-1 shows a block diagram of a standalone 5620 SAM system and the network that it manages. The management network, which contains the 5620 SAM components, connects to the managed network of NEs from one or more points, depending on the deployment complexity.

Figure 1-1 Standalone 5620 SAM system



A 5620 SAM operator performs network management or system administration tasks using a GUI or OSS client that connects to a main server. The main server sends and receives NE management traffic, and directs optional auxiliary servers to perform intensive tasks such as NE statistics collection. Main and auxiliary servers store information in the same 5620 SAM database.

The 5620 SAM uses a Java-based technology that provides distributed, secure, and scalable processing. See the *5620 SAM System Architecture Guide* for system design information. See chapter 7 for information about 5620 SAM system redundancy.

1.2 About this guide

The *5620 SAM User Guide* describes the various 5620 SAM functions, explains the GUI operations associated with each function, and indicates whether the function is available through the OSSI. See the *5620 SAM XML OSS Interface Developer Guide* for information about using the OSSI to perform a 5620 SAM function.

5620 SAM User Guide procedures that contain configurable parameters have links to parameter descriptions in the *5620 SAM Parameter Guide*, where appropriate.

Note — The *5620 SAM User Guide* parameter links can function only when the *5620 SAM Parameter Guide* is in the same directory as the *5620 SAM User Guide*.

This guide contains the following volumes, which are ordered by functional area, from lowest to highest:

- Introduction—contains general 5620 SAM information such as the following:
    - a system overview
    - feature lists by release
    - basic GUI operation instructions
    - GUI map management
- 5620 SAM system management—contains information about 5620 SAM administration such as the following:
    - system configuration
    - system redundancy
    - system and user security
    - interworking with other systems
- Device management—contains information about device functions that are not directly related to networking, such as the following:
    - device support
    - preparing devices for 5620 SAM management
    - 5620 SAM device and equipment management functions
- Network management—contains information about network functions such as the following:
    - general routing and forwarding
    - protocol-specific routing and forwarding
    - traffic management using MPLS and service tunnels
    - fault management
    - OAM diagnostic tests
    - NE redundancy
- Policy management—contains information about configuring and applying 5620 SAM policies that define rules for NE, network, or 5620 SAM operation
- Service management—contains information about managing customer services, such as the following:
    - service creation and configuration
    - customer and subscriber management
    - service verification, troubleshooting, and root-cause analysis
    - scheduling of routine, service-related operations

1.3 Workflow for network management using the 5620 SAM

The following workflow describes the sequence of high-level tasks required to deploy the 5620 SAM and use it to perform network management.

You can use an OSS client to perform many of the functions described in this workflow. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

You can use scripts and templates to perform complex CLI configuration of managed devices from the 5620 SAM. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Plan your 5620 SAM deployment by considering things such as the following:

- the number of NEs the 5620 SAM is to manage
- the hardware required for the 5620 SAM system
- the redundancy requirements
- management network latency
- management network bandwidth requirements
- naming conventions for 5620 SAM objects that you create
- NE compatibility with the 5620 SAM software

See the *5620 SAM Planning Guide* and the *5620 SAM Network Element Compatibility Guide* for more information.

2 Install the 5620 SAM software, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

3 Become familiar with GUI basics such as the following:

- navigating the GUI, using the GUI elements, and performing searches; see chapter 3 for more information
- using the equipment navigation tree; see chapter 4 for more information
- using topology maps; see chapter 5 for more information

4 As required, customize or configure the 5620 SAM operating environment.

a See chapter 6 for information about the following:

- viewing or changing 5620 SAM license information; see section 6.2 for more information
- using the auto-client update utility to define the configuration of each GUI client; see section 6.3 for more information
- securing 5620 SAM server/database communication; see section 6.3 for more information
- changing global network-management operating parameters; see section 6.4 for more information

b Manage 5620 SAM system redundancy; see chapter 7 for more information.

c Configure database logging, and manage other database administration functions such as backup and restore; see chapter 8 for more information.

d Create 5620 SAM user groups and accounts with privileges for specific operational scopes; see chapter 9 for more information.

e Configure SSL security for the 5620 SAM system; see chapter 10 for more information.

f Configure integration for the 5620 SAM and external systems such as the 5620 NM, the 5650 CPAM, and the 5780 DSC; see chapter 11 for more information.

5 Prepare the network devices for 5620 SAM management.

a Become familiar with the support that the 5620 SAM provides for various devices; see chapter 12 for more information.

b Commission devices for 5620 SAM management, and configure how and when the 5620 SAM polls the devices for MIB changes; see chapter 13 for more information.

c If required, perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

d If required, use a Telnet or SSH CLI from the 5620 SAM to view and modify device configurations; see chapter 15 for more information.

6 Use the 5620 SAM to manage devices.

a View, manage, and configure equipment navigation tree objects such as the following:

- network objects; see chapter 16 for more information
- device objects; see chapter 17 for more information
- logical group objects; see chapter 18 for more information
- shelf, card, and daughter card objects; see chapter 19 for more information
- port and channel objects; see chapter 20 for more information

b Create equipment inventories of managed devices; see chapter 22 for more information.

c Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21 for more information.

d If required, configure TCP enhanced authentication between NEs; see chapter 24 for more information.

e Perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

f Perform additional device management functions such as the following:

- card migration; see chapter 25 for more information
- threshold crossing alert policy management; see chapter 26 for more information
- bulk configuration changes; see chapter 27 for more information
- object life cycle management; see chapter 28 for more information
- automatic provisioning; see chapter 29 for more information

7 As required, use the 5620 SAM to manage network functions.

a Configure basic NE routing and forwarding; see chapter 30 for more information.

b Configure NE protocols; see chapter 31 for more information.

c Configure MPLS and LSPs; see chapter 32 for more information.

d Configure service tunnels to carry service traffic; see chapter 33 for more information.

e Configure NE-specific network functions such as the following:

- Lawful Intercept; see chapter 34 for more information
- IPsec; see chapter 35 for more information
- ISA-Video; see chapter 36 for more information

f Configure 5620 SAM alarm policies, and use alarms to perform fault management; see chapter 37 for more information.

g Use OAM diagnostic tools to troubleshoot network problems; see chapter 38 for more information.

h Configure redundancy in the managed network using functions such as the following:

- VRRP; see chapter 39 for more information
- APS; see chapter 40 for more information
- MC peer, endpoint, LAG, synchronization, and ring groups; see chapters 41 to 45 for more information

8 Create 5620 SAM policies that define the conditions for 5620 SAM management functions that include the following:

- network—ACL filters, auto-tunnel, RMON
- service—QoS, multicast traffic management, residential subscriber
- 5620 SAM—time of day, size constraint, format and range

See chapter 46 for general information about 5620 SAM policy management. See chapters 47 to 63 for information about specific policy types.

9 Use the 5620 SAM to manage customer services and related functions.

a Become familiar with 5620 SAM service management concepts such as SAPs, the TPSDA model, and QoS delivery using shared queue groups; see chapters 64 and 65 for more information.

b Configure and manage virtual ports; see chapter 66 for more information.

c Configure and manage customers; see chapter 67 for more information.

d Configure and manage the residential subscribers of customer services; see chapter 68 for more information.

e Configure VLAN services for subscribers connected to 7250 SAS or Telco devices; see chapter 69 for more information.

f Configure VLL Apipe, Cpipe, Epipe, Fpipe, Ipipe, and Hpipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information.

g Configure VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information.

h Create mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information.

i Configure IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information.

j Configure VPRN services to provide a virtual IP network that connects multiple customer sites; see chapter 74 for more information.

k Interconnect customer sites that span different domains, such as MAN-WAN or Inter-AS; see chapter 75 for more information.

l Configure composite services to connect various types of services; see chapter 76 for more information.

m Configure Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 77 for more information.

n Configure 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information.

o Use the 5620 SAM Service Test Manager to group OAM diagnostic tests into suites of manual and automatically-generated tests; see chapter 78 for more information.

p Configure Ethernet CFM to detect, isolate, and report connectivity faults in Ethernet networks; see chapter 80 for more information.

q Use the RCA audit tool to perform on-demand verifications of the configuration of services and physical links; see chapter 81 for more information.

10 Collect 5620 SAM and NE statistics to monitor 5620 SAM, network and service performance, compile equipment usage and billing data, and ensure SLA compliance; see the *5620 SAM Statistics Management Guide* for more information.

2 — 5620 SAM features

2.1 New for 5620 SAM Release 9.0 R7

Table 2-1 lists the features and functions added in 5620 SAM Release 9.0 R7.

Table 2-1 5620 SAM Release 9.0 R7 features

Feature or function	Description	Reference for more information
GUI enhancements		
—	—	—
Map enhancements		
Discovered physical link referencing	Support for manual referencing and unreferencing of physical links discovered through LLDP or the 5650 CPAM.	See Procedure 5-38 for more information.
5620 SAM System management enhancements		
—	—	—
Device management enhancements		
Sync alarm and alarm aggregation on GNE	GNE alarm catalogue supports GNE MTIE Alarm type. The system can raise an alarm on a GNE using System Address and/or Interface Index varbind positions.	See Chapter 13 for more information.
7210 SAS-D enhancements		
Synchronous Ethernet	The 7210 SAS-D Release 3.0 R6 supports the configuration of synchronous Ethernet.	See Procedures 20-1 and 19-24 for more information.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, and 7210 SAS-X enhancements		
SAA accounting files	The 7210 SAS-D Release 4.0 R1 and later, the 7210 SAS-E Release 4.0 R1 and later, the 7210 SAS-M Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 support the configuration and distribution of the SAA accounting record type.	See Procedure 78-4 for more information.
7210 SAS-M enhancements		
IGMP snooping	The 7210 SAS-M Uplink Release 4.0 R1 and later supports IGMP snooping.	See Procedure 71-2 and 71-3.
7210 SAS-M and 7210 SAS-X enhancements		
Port loopback	The 7210 SAS-M Release 3.0 R6 and later, and the 7210 SAS-X Release 3.0 R6 and later support the configuration of timed loopback type parameter on Ethernet ports.	See Procedure 20-1 for more information.
Split horizon groups	The 7210 SAS-M Network Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of split horizon groups, which can be bound to ports, VPLS L2 access interfaces, and spoke SDP bindings.	See Procedures 20-1, 20-14, 20-16, 71-3, 71-5, 71-13, and 71-14 for more information.
Routing policy configuration	The 7210 SAS-M Network Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of Community, Damping, and AS Path routing policies.	See Procedures 30-13 to 30-15 for more information.
BGP site configuration	The 7210 SAS-M Network Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the creation of BGP sites.	See Procedures 31-1 to 31-6 for more information.

(1 of 5)

Feature or function	Description	Reference for more information
Ethernet sub-ring enhancements	The 7210 SAS-M Release 4.0 R2 and later, and the 7210 SAS-X Release 4.0 R2 and later support the creation of Ethernet sub-rings with interconnections.	See Procedures 33-5 and 33-7 for more information.
VPRN configuration	The 7210 SAS-M Network Release 4.0 R2 and later, and the 7210 SAS-X Release 4.0 R2 and later support the following VPRN functions: • configuration of VPRN OAM diagnostics • creation of VPRN services • creation of VPRN L3 Access Interfaces • configuration of BGP on VPRN routing instances • creation of spoke SDP bindings on VPRN services • collection of various statistics on VPRN services	See Procedures 38-14, 74-1, 74-2, 74-5, and 74-10 for more information.
7210 network policy enhancements	The 7210 SAS-M Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of additional ingress parameters on network interface type network policies.	See Procedure 47-7 for more information.
7450 ESS and 7750 SR enhancements		
ISA TMS daughter card support	The 5620 SAM supports the ISA TMS daughter card on the 7750 SR-7 and 7750 SR-12, Release 9.0 R5 or later. Mixed mode is not supported on the ISA TMS daughter card.	See chapter 19 for more information.
7705 SAR enhancements		
VLL Hpipe service	The 5620 SAM supports VLL Hpipe service on DS1 ASAP MDA and 7705 SAR-M. Supported in 7705 SAR, Release 5.0 R1 and later.	See chapter 70 for more information.
MDA Mode	The 5620 SAM supports two MDA modes for channelized ASAP MDAs and two MDA modes for the 10-port 1GigE 1-port 10GigE X-Adapter card.	See MDA modes for the 7705 SAR in chapter 19 and Procedure 19-24 for more information.
Graceful restart and helper mode for OSPFv2	The 5620 SAM supports graceful restart and helper mode options on OSPFv2 routing instances.	See Procedure 31-22 for more information.
STP for MVPLS	The 5620 SAM supports spanning tree protocol for MVPLS L2 access interfaces. Supported on the 7705 SAR, Release 5.0 R1 or later.	See Procedure 71-3 for more information.
Fpipe enhancements	The 5620 SAM supports FR encapsulation on the following 7705 SAR-8/18 MDAs: • 16/32 x Channelized DS1/E1 ASAP v2 • 4 x Channelized DS3/E3 ASAP • 12 x Serial Data configured with X.21 or V.35 serial types	See MDA modes for the 7705 SAR in chapter 19 and Procedure 70-6 for more information.
	The 5620 SAM supports FR encapsulation on the i16 x Channelized DS1/E1 ASAP on the 7705 SAR-M.	See MDA modes for the 7705 SAR in chapter 19 and Procedure 70-6 for more information.

(2 of 5)

Feature or function	Description	Reference for more information
Ipipe enhancements	The 5620 SAM supports Ipipe services on ports configured for FR encapsulation.	See Procedure 70-8 for more information.
	The 5620 SAM supports IPCP encapsulation on OC3 channels of the 2 x Channelized OC3/STM1 ASAP SFP card.	See chapter 20 for more information.
	The 5620 SAM supports Ipipe services on ports configured for cHDLC encapsulation on DS1/E1 MDAs. Supported in 7705 SAR Release 5.0 R1 and later.	See MDA modes for the 7705 SAR in chapter 19 and Procedure 70-8 for more information.
	The 5620 SAM supports two configurable SAPs on an Ipipe service on the 7705 SAR Release 5.0 R1. SDP bindings cannot be bound to SAPs on Ipipe services that support two SAPs.	See Procedure 70-8 for more information.
Apipe enhancements	The 5620 SAM supports SAP aggregation groups on 7705 SAR Apipe services.	See Apipe (ATM VLL) in chapter 70, Procedure 70-4, and Procedure 70-14 for more information.
	The 5620 SAM supports the ATM N:1-N>1 VC type, allowing for interoperability to create a single Apipe service using SAP aggregation groups on a 7705 SAR Apipe service and connection profiles on a 7750 SR Apipe service.	See Apipe (ATM VLL) in chapter 70, Procedure 70-4, and Procedure 70-14 for more information.
	The 5620 SAM supports ATM encapsulation on E3 channels configured on the 4 x Channelized DS3/E3 ASAP card on the 7705 SAR-8/18, Release 5.0 R1 or later.	See MDA modes for the 7705 SAR in chapter 19 and Procedure 70-4 for more information.
Cpipe enhancements	The 5620 SAM supports Cpipe services on DS3, E3, and OC3 channels configured for CEM encapsulation.	See MDA modes for the 7705 SAR in chapter 19 and Procedure 70-9 for more information.
Service retargeting	The 5620 SAM supports copy and move functions for 7705 SAR SAPs on Cpipe, Hpipe, Fpipe, and Ipipe services.	See Procedure 20-5 for more information.
VPRN enhancements	The 5620 SAM supports eBGP on VPRN instances on the 7705 SAR, Release 5.0 R1 or later.	See Procedure 74-5 for more information.
VPLS MC QoS	The 5620 SAM supports configuring access ingress and network ingress aggregate rates on the 7705 SAR-M.	See Procedure 17-13 for more information.
Auxiliary alarm enhancements	The 5620 SAM supports configuring auxiliary alarm digital inputs as normally open or normally closed.	See Procedure 19-9 for more information.
LAGs	The 5620 SAM supports link aggregation groups on the 7705 SAR-8/18, Release 5.0 R1 or later. LAGs on the 7705 SAR can contain no more than two links and can be configured only on access ports.	See Procedure 18-13 for more information.
IEEE 1588 PTP transparent clock	The 5620 SAM supports end-to-end transparent clocks for IEEE 1588 PTP on the 7705 SAR-M/ME.	See IEEE 1588 PTP clock in chapter 19 and Procedure 19-6 for more information.
Differential clock recovery	The 5620 SAM supports differential clock recovery on the 7705 SAR-M/ME, Release 5.0 R2 or later.	See Procedures 20-40 and 20-41 for more information.
DS1 channels	The 5620 SAM supports DS1 channels on the 2 x Channelized OC3/STM1 ASAP SFP MDA.	See chapter 20 for more information.
SDI and 6 x EM for 7705 SAR-18	The 5620 SAM supports the SDI and 6 x EM cards on the 7705 SAR-18.	See 7705 SAR 12-port SDI card and 7705 SAR six-port E&M daughter cards in chapter 12, Procedure 20-13, and Procedure 20-42 for more information.
Sub-rate speeds for SDI	The 5620 SAM supports sub-rate speeds for RS232 and X.21 serial types.	See Procedure 20-42 and the Speed parameter description for more information.

(3 of 5)

Feature or function	Description	Reference for more information
Power Injector card	The 5620 SAM supports the Microwave Power Injector card on the 7705 SAR-8/18 at beta level.	See 7705 SAR Power Injector card in chapter 12 for more information.
8-port Ethernet SFP card	The 5620 SAM supports the 8-port 10/100/1000 Ethernet SFP card on the 7705 SAR-8/18 at beta level.	See chapter 12 for more information.
10-port 1GigE/1-port 10GigE X-Adapter card	The 5620 SAM supports the 10-port 1GigE/1-port 10GigE X-Adapter card. This card is supported on the 7705 SAR-18 and can be configured to operate with ten 1-gigabit ports or with one 10-gigabit port at beta level.	See 7705 SAR 10-port 1GigE/1-port 10GigE X-Adapter card in chapter 12 and MDA modes for the 7705 SAR in chapter 19.
1, 2, 4, and 8-colour Optical Add/Drop Mux card	The 5620 SAM supports the OADM card in 1, 2, 4, and 8-colour variants on the 7705 SAR-8/18.	See 7705 SAR Optical Add/Drop Mux cards in chapter 12 for more information.
7705 SAR-M/ME	The 5620 SAM supports the 7705 SAR-M/ME node with variant chassis, integrated cards, and a module card slot.	See 7705 SAR-M daughter cards chapter 12 for more information.
7705 SAR-M/ME expansion module MDAs	The 5620 SAM supports the following plug-in module MDAs on the 7705 SAR-M/ME: • GPON module • DSL module • DSL combo module (DCM) • 1 Colour Optical Add/Drop Mux module (OADM)	See 7705 SAR-M daughter cards in chapter 12 and Procedure 19-27 for more information.
7705 SAR-8 v2 chassis	The 5620 SAM supports the 7705 SAR-8 v2 chassis.	See chapter 12 for more information.
9500 MPR enhancements		
ERP (G.8032) support	Support for configuring Ethernet Ring Protection (G.8032) on the 9500 MPR, Release 3.1 or later devices. ERP provides rapid detection and recovery time if a link or node fails.	See chapters 12 and 33 for more information.
EVPL mode on 9500 MPR (dot1q) VLAN services	Support for configuring the EVPL mode on 9500 MPR (dot1q) VLAN services. This allows you to configure a Point to Point VLAN service between 9500 MPR NEs.	See Procedure 69-8 for more information.
NEtO support enhancement	Support for opening NEtO sessions using the 5620 SAM GUI for the 9500 MPR, Release 3.3, has been added and simplified.	See Procedure 13-15 for more information.
OmniSwitch enhancements		
—	—	—
Network management enhancements		
—	—	—
Protocol enhancements		
—	—	—
Policy enhancements		
Auto tunnel enhancement	Support for the Import Administrative Groups parameter on Auto Tunnel rules for SDP tunnels.	See chapter 52 for more information.
SLA profile enhancements	Support for new ingress and egress report-rate parameters on SLA profiles.	See Procedure 68-13 for more information.
Service management enhancements		

(4 of 5)

Feature or function	Description	Reference for more information
Enumerated forwarding class values for OAM tests	When you mouse over the drop-down list of Forwarding Class parameter options on the Test Parameters tab of an OAM test configuration form, a tool tip displays the numeric value of each forwarding class. Also, in test results sent to the OSSI, the 5620 SAM returns the numeric forwarding class value in addition to the alphanumeric identifier.	—
VLAN customer configurable	You can choose the customer associated with a VLAN service after service creation.	—
Option to populate device site name with service name	You can enable a global 5620 SAM option that populates the service site name property on an NE using the service name when an NE is added as a service site.	See chapter 67 for more information.
Additional features		
—	—	—
5620 SAM documentation enhancements		
—	—	—
Discontinued support		
—	—	—

(5 of 5)

2.2 5620 SAM Release 9.0 R6

5620 SAM Release 9.0 R6 is a maintenance release. No features have been added.

2.3 5620 SAM Release 9.0 R5

Table 2-2 lists the features and functions added in 5620 SAM Release 9.0 R5.

Table 2-2 5620 SAM Release 9.0 R5 features

Feature or function	Description	Reference for more information
GUI enhancements		
Search message	For lists that do not populate automatically, the message “Press "Search" to populate list.” displays in the result panel when you first open the list form.	See section 3.2 for more information.
Search filters	The search filter DOES NOT CONTAIN is added to allow more precise filtering of text strings, IP addresses, and MAC addresses.	See Using search filters in chapter 3 for more information.
Equipment group filters	You can filter when you search for new alarms, historical alarms, managed equipment objects, and managed service objects by equipment that is organized by topology group.	See Equipment group filters in chapter 3 for more information.

(1 of 9)

Feature or function	Description	Reference for more information
Apply changes to object-level tabs on configuration forms	The Apply Tab button is added to the NE and composite services configuration forms. On these forms, changes implemented by pressing the Apply Tab button apply only to the current object-level tab.	See Modified configuration forms in chapter 3 for more information.
Configuration form enhancements for composite services	The following 5620 SAM client GUI configuration form enhancements are extended to the composite services configuration form: • the navigation tree is now on the left side of composite service configuration forms, for improved object accessibility • the ability to undock configurable object forms from the main composite service configuration form window	—
Equipment Window form no longer supported	The Equipment Window form has been removed from the 5620 SAM client GUI. Information that was previously accessible through the Equipment Window continues to be accessible from object properties forms. The graphical representation of a device shelf is accessible from the Shelf object on the navigation tree. Detailed inventory information is accessible from the Inventory tab on the NE configuration form.	See section 19.2 for more information about accessing the graphical representation of a device. See chapter 22 for more information about accessing inventory information.
General configuration form enhancement	A More Actions button has been added to all configuration forms. Clicking the More Actions button displays a contextual menu of configuration form options.	—
Mandatory field or incorrect data indicator	The asterisk indicator is extended to script and template configuration forms.	—
Scripts shortcut	The introduction of this shortcut allows users with the appropriate scope of command roles to associate scripts and templates to object types directly from the navigation tree, map objects, or the configuration form without having to navigate through the Script Manager.	See Table 4-2 in chapter 4 for more information about the Scripts shortcut option.
New default topology group	Newly added unmanaged network elements appear in a topology group called Unmanaged NEs. You can drag and drop unmanaged network elements from this topology group to any other group on the topology map or in the navigation tree.	See chapter 16 for more information.
Map enhancements		
Alarmed links/All links button enhancement	The ability to display specific links with associated alarms is added to the All links shown button.	See Table 5-1 in chapter 5 for more information.
5620 SAM System management enhancements		
—	—	—
Device management enhancements		
Vendor-specific ICMP extensions	The ability to configure vendor-specific ICMP extensions is extended to the 7450 ESS, 7710 SR, and 7750 SR device types.	See Procedure 17-12 for more information.
New alarm for 7450 ESS, 7710 SR, and 7750 SR nodes	The Configuration Roll Back Status alarm has been introduced for the 7450 ESS, 7710 SR, and 7750 SR nodes Release 9.0 R4 and later.	See the *5620 SAM Alarm Reference* for more information.
7210 SAS-D enhancements		
Y.1731 Ethernet OAM	The 7210 SAS-D Release 3.0 R5 and later supports EthTest, One Way Delay, and Two Way Delay.	See Procedure 18-13 for more information.

(2 of 9)

Feature or function	Description	Reference for more information
Synchronous Ethernet	The 7210 SAS-D 6F 4T ETR Release 3.0 R5 and later supports the configuration of timing synchronization.	See Procedure 19-5 for more information.
Port Clock Mode	The 7210 SAS-D Release 3.0 R5 and later supports the configuration of a new Port Clock Mode parameter on Ethernet ports.	See Procedure 20-1 for more information.
Ethernet Ring Protection	The 7210 SAS-D Release 3.0 R5 and later supports the configuration of Ethernet Ring Protection.	See Procedures 33-7 and 33-10 for more information.
IGMP Snooping	The 7210 SAS-D Release 3.0 R5 and later supports IGMP Snooping.	See Procedure 71-2 for more information.
7210 SAS-D and 7210 SAS-E enhancements		
Port Threshold in LAG	The 7210 SAS-D Release 3.0 R5 and later, and the 7210 SAS-E Release 3.0 R5 and later support the configuration of Port Threshold parameters when creating a LAG.	See Procedure 18-13 for more information.
MSTP	The 7210 SAS-D Release 3.0 R5 and later, and the 7210 SAS-E Release 3.0 R5 and later support the creation of MSTP sites for an MVPLS.	See Procedure 71-10 for more information.
7210 SAS-D, 7210 SAS-E, and 7210 SAS-M enhancements		
IP MTU	The 7210 SAS-D Release 3.0 R5 and later, the 7210 SAS-E Release 3.0 R5 and later, and the The 7210 SAS-M Uplink Release 3.0 R5 and later support the configuration of IP MTU on L3 access interfaces.	See Procedures 20-1 and 73-1 for more information.
7210 SAS-D, 7210 SAS-E, 7210 SAS-M, and 7210 SAS-X enhancements		
Accounting policy statistics collection	The 7210 SAS-D, the 7210 SAS-E, the 7210 SAS-M, and the 7210 SAS-X support the collection of accounting policy statistics.	See the *5620 SAM Statistics Management Guide* for more information.
7210 SAS-D and 7210 SAS-M enhancements		
Transit SAPs	The 7210 SAS-D Release 4.0 R1 and later, and the 7210 SAS-M Uplink Release 4.0 R1 and later support the configuration of transit SAPs for VPLS and Epipe services.	See Procedures 70-2 and 71-2 for more information.
IP Interface for VPLS service	The 7210 SAS-D Release 3.0 R5 and later, and the 7210 SAS-M Uplink Release 3.0 R5 and later support IP Interfaces for VPLS service.	See Procedure 71-2 for more information.
7210 SAS-M and 7210 SAS-X enhancements		
MC LAG	The 7210 SAS-M Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of MC Peer, MC LAG, and MC Sync.	See chapters 41, 43, and 44 for more information.
7210 Port Access Egress policies enhancements	The 7210 SAS-M Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support additional options for the configuration of 7210 Port Access Egress policies.	See Procedure 47-4 for more information.
7210 MPLS LSP-Exp Map policy configuration	The 7210 SAS-M Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of 7210 MPLS LSP-Exp Map policies.	See Procedure 47-26 for more information.
PBB	The 7210 SAS-M Network Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of PBB on B-VPLS, I-VPLS, and Epipe services.	See Procedures 70-2, 71-11, and 71-12 for more information.
PW Redundancy	The 7210 SAS-M Network Release 4.0 R1 and later, and the 7210 SAS-X Release 4.0 R1 and later support the configuration of PW Redundancy on a VPLS service.	See Procedures 71-1 and 71-5 for more information.

(3 of 9)

Feature or function	Description	Reference for more information
7450 ESS and 7750 SR enhancements		
New daughter card support	The 5620 SAM supports the following new daughter cards: • 4 x ATM OC12/OC3 SFP B on the 7750 SR, Release 9.0 R6 or later and on the 7450 ESS, Release 9.0 R6 or later • 16 x ATM OC3 SFP B on the 7750 SR, Release 9.0 R6 or later and on the 7450 ESS, Release 9.0 R6 or later • 16 x OC12/OC3 SFP B on the 7750 SR, Release 9.0 R4 or later and on the 7450 ESS, Release 9.0 R4 or later • 4 x OC48 SFP B on the 7750 SR, Release 9.0 R4 or later and on the 7450 ESS, Release 9.0 R4 or later In addition to supporting the functions on the existing non-B version of the daughter card, these new daughter cards support the configuration of loop-timing on a per-port basis.	See chapter 19 for more information.
Extended WAN-PHY support	Configuration of an Ethernet interface as a WAN-PHY interface is extended to the 12-port 10-Gbyte Magma IMM. WAN-PHY is configured using the XGig Mode parameter.	See chapter 20 for more information.
Stateless APS switchover	Support for the Stateless Aps Switchover parameter, which is configurable for MLPPP APS bundles.	See the *5620 SAM Parameter Guide* for more information.
7705 SAR enhancements		
7705 SAR-M 5.0 support at 7705 SAR 4.0 feature parity	Support for the 7705 SAR-M 5.0, with feature support at parity with the 7705 SAR 4.0. Includes the 7-port Ethernet card and 16-port ASAP card.	See chapter 12 for more information.
9500 MPR enhancements		
Multiple radio links support	Support for multiple radio links between two 9500 MPR devices.	See chapter 13 for more information.
VLAN path creation and management enhancements	The 5620 SAM extends the existing manual VLAN path management to automate the process of creating VLAN paths for redundant and non-redundant configurations. Three VLAN creation options are now available: manual, automatic, and point 2 point.	See chapter 70 for more information.
Configuration of TDM ports on 9500 MPR cards	You can only configure the administrative state of TDM ports on the following 9500 MPR cards when the Signal mode parameter associated with the port is set to an option other than disabled. • 32 x E1 (ETSI) • 32 x DS1(ANSI) • 16 x E1 ASAP Access (ETSI) • 2 x DS3 (ANSI) This functional change was made so the default administrative state of the TDM ports is IETF compliant.	See chapter 12 for more information.

(4 of 9)

Feature or function	Description	Reference for more information
LAG object support	LAG object support for the following ports in 9500 MPR Release 3.1.0: • MPT-HC • MPT-MC • MPT-HL LAG object support for the following ports in 9500 MPR Release 3.2.0: • MPT-HC • MPT-MC • MPT-HL • MD300 • Ethernet	See section 12.19 for more information.
Port segregations for LAGs	You can segregate ports from one LAG to another and from one LAG to another port.	See Procedure 20-27 for more information.
Core-enhanced card enhancements	The 5620 SAM supports the direct connection of MPT radio ports on core-enhanced cards on the ETSI and ANSI 3.1.0 or later of 9500 MPR devices. MPT-HC, MPT-HCv2, MPT-MC, and SFP are supported.	See chapter 12 for more information.
MPT-HCv2 support	The 5620 SAM supports MPT-HCv2 for 2+2 x Ethernet (EAS) cards and core-enhanced cards.	See chapter 12 for more information.
4+4 x Ethernet (EAS) card enhancements	The 4+4 x Ethernet (EAS) card with MPT-HL support can be configured on any card slot on the 9500 MPR ANSI 3.1 or later.	See chapter 12 for more information.
2+2 x Ethernet (EAS) card enhancements	The 5620 SAM supports the 2+2 x Ethernet (EAS) card with MPT-HC and MPT-MC support for ANSI 3.1 or later.	See chapter 12 for more information.
Service-in-service automatic discovery	The 5620 SAM now automatically associate a transport service with a newly discovered service tunnel when a physical link is created between a 9500 MPR and a non-MPR NE.	See chapter 70 for more information.
Power level performance management enhancements	Additional statistics have been added for power level performance management and plotter functions for: • Hop Current Data Stats • Link Current Data Stats • RSL Hop Current Data Stats • HSL Hop Current Data Stats	See Procedure 20-28 for more information. See the *5620 SAM Statistics Management Guide* for more information on plotter functions.
SDH 1+1 protection and card support for ETSI 3.1 and later	Support for 2xSTM card with SFP-O and SFP-E for ETSI 3.1 and later.	See Procedure 20-22 for more information.
SDH channelized and protection support for ETSI 3.1 and later	Support for 1xSTM channelized card with SFP-O and SFP-E for ETSI 3.1 and later.	See Procedure 20-23 for more information.
Radio and Ethernet LAG support	Support for Radio and Ethernet LAG Aggregation type.	See Procedure 18-17 for more information.
XPIC (1+1 redundancy)	XPIC is an ODU which draws power and data from a 2+2 EAS card when the port is configured as MPT-HC.	See chapter 12 for more information.
QoS configuration	The 5620 SAM provides QoS configuration support on the 9500 MPR. The 9500 NE QoS policy supports mapping and global queue settings and the 9500 Radio Interface Queue Map policy supports queue size settings of the radio interface.	See Procedures 47-33 and 47-34 for more information.

(5 of 9)

Feature or function	Description	Reference for more information
NE date and time configuration	The 5620 SAM provides NE date and time configuration on the 9500 MPR.	See Procedure 17-2 for more information.
OmniSwitch enhancements		
OmniSwitch 10K support	The 5620 SAM supports the OS 10K Modular Ethernet LAN switch. The switch has a 12-slot chassis configuration with Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet capabilities.	See chapter 12 for more information.
OmniSwitch 6900 support	The 5620 SAM supports the OS 6900 family of standalone aggregation switches that consists of two models: the OS 6900-X40 (1.28 Tb/s) and the OS 6900-X20 (640 Gb/s).	See chapter 12 for more information.
LLDP support	Support for LLDP on the OS 10K and OS 6900.	See Procedures 17-9 and 20-34 for more information.
LAG support	Support for the creation of LAGs on the OS 10K and OS 6900.	See Procedure 18-16 for more information.
Ethernet port configuration support	Support for the configuration of Ethernet ports on the OS 10K and OS 6900.	See Procedure 20-34 for more information.
OAM VLAN service support	Support for performing OAM diagnostic tests from the service topology view has been added for all OmniSwitch devices which support VLAN services except for enterprise (SME) OS 6250 devices. Tests supported include: continuity checking, loopbacks, one-way delay, two-way delay, and CFM link trace.	See chapters 38 and 80 and for more information.
Network management enhancements		
Advanced JMS message filters	You can create advanced filters to reduce the number of JMS event messages sent to OSS clients. An advanced JMS message filter is a 5620 SAM-O XML filter that specifies the following: • the types of event notifications that are to be sent to the client • a set of object properties to use as match criteria for messages sent to the client	See the *5620 SAM XML OSS Interface Developer Guide* for more information.
registerLogToFile supports performance statistics export	You can use the 5620 SAM-O registerLogToFile method to export performance statistics, in addition to accounting statistics.	See the *5620 SAM XML OSS Interface Developer Guide* and *5620 SAM Statistics Management Guide* for more information.
registerSasLogToFile supports retrieval of OAM logs	You can use the 5620 SAM-O registerSasLogToFile method to retrieve OAM logs that are based on specific class types.	See chapter 38 for more information.
Script cascading	You can use the 5620 SAM Script Manager to organize scripts in logical groups, or bundles, which permit interoperation between scripts in the bundle, or cascading. Scripts in a bundle can pass parameters to, and call, other scripts in the same bundle.	See the *5620 SAM Scripts and Templates Developer Guide* for more information.
Script scheduling	You can use the 5620 SAM to schedule script execution.	See the *5620 SAM Scripts and Templates Developer Guide* for more information.
TCA enhancements	The TCA function improvements include the following: • profile configuration for ease of management • custom threshold creation • delta threshold configuration	See chapter 26 for more information.

(6 of 9)

Feature or function	Description	Reference for more information
1+1 optimized APS groups	You can configure an SC APS group as 1+1 optimized. This architecture is optimized for networks which use predominantly bidirectional switching.	See chapter 40 for more information.
Create All Channel Support for APS Groups	Create All Channel is extended to APS and MC-APS port.	See chapter 20 and 40 for more information.
Querying network resources	Support added to view current network resources such as IP addresses, RDs and RTs, and MAC addresses.	See Procedure 30-1 for more information.
Protocol enhancements		
BGP Add-Path	You can configure a BGP site, group, or peer to send and receive BGP Add-Path route advertisements. Routers configured for BGP Add-Path will retain multiple paths to a single destination in its routing table.	See chapter 31 for more information.
PPPoA and PPPoEoA support	The 5620 SAM supports the configuration of PPPoA and PPPoEoA network protocols.	See Procedures 19-24, 66-2, 68-5, 68-20, 68-4, 68-35, 73-8, and 74-14, for more information.
Policy enhancements		
NE Management Access Filters enhancements	The 5620 SAM supports the configuration of new Log and Router parameters when creating IPv4 and IPv6 entries for NE Management Access Filters.	See Procedure 21-1 for more information.
Service management enhancements		
Service path search enhancements	Support for multi-segment tunnel selection and redundant path selection functionality.	See chapter 64 for more information.
Link LDP hello adjacency tracking	Support for Enable Fast Re-route parameter on LDP sites, and Enable BFD Tracking parameter on LDP interfaces. Support for Enable Loop-free Alternate parameter on ISIS sites.	See chapter 31 for more information.
Validation function for composite services	A test suite can now be used to validate a composite service.	See Procedure 76-3 for more information.
MS PW routing	Support for Multi-segment pseudo-wire routing to provide solutions for inter-domain services by using dynamic MS PW routing and signaling.	See chapter 75 for more information.
Tunnels for services	The concept of a service tunnel has been broadened to include services acting as tunnels as well.	See chapter 33 for more information.
Ethernet CFM Up MEP SAP generation for Epipe and VPLS	End-to-end test suite generation is now available for VPLS and VLL Epipe services.	See chapter 80 for more information.
GARP configuration on SRRP instances	New FIB Population Mode parameter for SRRP instances on IES and VPRN group interfaces.	See chapters 73 and 74 for more information
Usage-based billing	Usage-based billing groups can be enabled at the application profile level and associated with application groups and applications for application reporting to the 5670 RAM.	See chapter 77 for more information.
Application performance reporting	Support for DCP summarization to add route configuration to AA reporting data.	See chapter 77 for more information.
Transit prefix policies	Transit prefix policies can be configured to specify network or subscriber IP addresses for the creation of transit subscribers.	See chapter 77 for more information.

(7 of 9)

Feature or function	Description	Reference for more information
AA enhancements	The following enhancements are added for AA support: • ISA-AA support for HTTP expression matching • ISA-AA support for X-Online-Host • AA is supported on the 7750 SR-c12 • AA is supported for mixed mode on the 7450 ESS • IPv6 is supported for AA • You can set the administrative state for AA protocol stats in order to enable or disable AA protocol stats collection for specific partitions • You can view application filter hit stats	See chapter 77 for more information.
HTTP error redirect policies	Support for HTTP error redirect templates and error codes.	See chapter 77 for more information.
Spoke SDP FEC support	Support for spoke SDP FEC configuration on VLL Epipe service.	See chapter 70 for more information.
QPPB support	Support for Forwarding Class Name and Forwarding Class Priority configuration on routing policy statements and static routes. QoS Route Lookup (IPv4 and IPv6) configuration on subscriber group interfaces on IES and VPRN, L3 access interfaces on IES and VPRN, and base router network interfaces.	See chapters 30, 73, and 74 for more information
Port down on CRC support	Detects internal hardware errors on Ethernet ports, disables the associated port, and raises an alarm. New Down on Internal MAC Tx Error parameter, as well as CRC SD threshold and CRC SF threshold parameters.	See chapter 20 for more information.
Packetization buffer size calculation on CEM SAPs	Addition of the Packetization Buffer (ms) parameter, which is configurable for a CEM SAP on a Cpipe service. The new parameter removes the need for customers to manually calculate the packetization buffer size.	See chapter 70 for more information.
MEG sub-groups	MEPs can be divided into logical groupings called MEG sub-groups which allow you to direct Ethernet CFM to specific areas of the system.	See chapter 80 for more information.
GNE service sites	GNEs can be configured as service site objects and service interface objects on the service configuration forms. Supported on all VLLs, all 9500 MPR VLLs, VPLS, MVPLS, VPRN, and IES.	See chapters 70, 71, 73, and 74 for more information
Shared Domain ID	The Maintenance Domain ID parameter specifies a unique Maintenance Domain ID that can be forced to an NE.	See chapter 70 for more information
Customized STM test settings locked	Test Suite test settings can be locked to prevent loss of customized configurations	See chapter 78 for more information
Over-subscription thresholds	Operator can configure new thresholds associated to the access and network pools (including named pools)	See chapter 19 for more information
LSP manual switchover commands	Operator can perform manual switchover of LSPs	See Procedure 32-17 for more information
VPRN indirection for edge resilience	A backup path capability was added to all levels of BGP and to VPRN	See chapters 31 and 74 for more information
SRRP enhancements for PPPoE redundancy and PPPoE dual chassis Redundancy with MCS	Allows redundant shelves to establish PPPoE sessions for subscriber management	See chapters 41, 73 and 74 for more information
Alarms for composite services	Allows user to enable alarm aggregation for composite services	See chapters 67 and 76 for more information

(8 of 9)

Feature or function	Description	Reference for more information
Additional features		
CLI command to display active card alarms	Addition of Alarm Management and Maximum Cleared Alarms parameters to NE properties form for the 7450 ESS, 7710 SR, and 7750 SR. The new parameters allow customers to view NE alarms through the CLI	See chapter 19 for more information.
Script Editor and GUI Builder enhancements	The collapsible panel functionality is extended to include the GUI builder and associated templates, and CLI and XML API configuration scripts.	See the *5620 SAM Scripts and Templates Developer Guide* for more information.
5620 SAM documentation enhancements		
New on-product help system	A new on-product help system consolidates all 5620 SAM user documentation, delivering customer documentation and resources in both HTML and PDF.	See Help→User Documentation on the 5620 SAM GUI
5620 SAM Alarm Reference	The *5620 SAM Alarm Reference* is a new document that consolidates the 5620 SAM alarms from the *5620 SAM Troubleshooting Guide* and other 5620 SAM documents. The alarms are organized in chapters, by device type.	See the *5620 SAM Alarm Reference*.
Discontinued support		
—	—	—

(9 of 9)

2.4 5620 SAM Release 9.0 R4

5620 SAM Release 9.0 R4 is a maintenance release. No features have been added.

2.5 5620 SAM Release 9.0 R3

Table 2-3 lists the features and functions added in 5620 SAM Release 9.0 R3.

Table 2-3 5620 SAM Release 9.0 R3 features

Feature or function	Description	Reference for more information
GUI enhancements		
Text messaging enhancements	The 5620 SAM GUI client text messaging has been enhanced to include: • Messages are now uniquely identified with the Client ID number of the message sender. • A reply function has been added taking the Client ID into account, so that an operator receiving a text message can send a response immediately.	See Procedure 3-23 for more information.
Objects added to navigation tree	The Fans and Power Supplies objects are added to the navigation tree NE objects. Fan and power supply object display is not supported for 1830 PSS NEs.	—

(1 of 5)

Feature or function	Description	Reference for more information
User switching	You can switch to a different 5620 SAM GUI user by choosing a main menu option.	See chapter 3 for more information.
Main menu changes for Layer 2 policies	The Policies→Layer2 menu has changed to Policies→Ethernet.	—
5620 SAM system management enhancements		
Automatic database backup file set compression	You can configure the 5620 SAM Database Manager to automatically gzip and tar a database backup file set, which eases file management and conserves disk space.	See chapter 8 for more information.
Increased database security	The 5620 SAM database user and Oracle SYS user password algorithms are enhanced to meet U.S. Department of Defense requirements.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about setting these passwords during a 5620 SAM system installation or upgrade. See the *5620 SAM Maintenance Guide* for information about changing the passwords after an installation or upgrade.
Remove empty services	System Preferences option to remove from the 5620 SAM any service objects that have no sites configured.	See chapter 67 for more information.
New CPM/Switch Fabric 4	The 500 Gb/s CPM/ Switch Fabric 4 is supported on the 7750 SR-7, and 7450 ESS-7. The 1 Tb/s CPM/Switch Fabric 4 is supported on the 7750 SR-7, 7750 SR-12, 7450 ESS-7, and 7450 ESS-12.	See chapter 17 for more information.
Device management enhancements		
DS0 group level channelization	Supports the automatic configuration of sub-channels and assignment of timeslots on port in DS0 groups.	See chapter 20 for more information
Consolidated view of DS0 group timeslot assignments	Supports a consolidated view of channels that are assigned in DS0 groups. You can disable, enable, or reassign the assignment of timeslots within a DS0 group using the associate properties form.	See chapter 20 for more information
Script locking	A 5620 SAM GUI operator can prevent other 5620 SAM users from executing, modifying, and deleting CLI script targets and XMLAPI instances created by the current user.	See the *5620 SAM Scripts and Templates Developer Guide* for more information.
New alarms for 1-Port 100GE CFM IMM	The following alarms have been introduced for the 1-Port 100GE CFM IMM— No AM Lock, No Block Lock, and Duplicate Lane.	See the *5620 SAM Troubleshooting Guide* for more information.
7210 SAS-M and 7210 SAS-X enhancements		
Timing enhancements	Quality level and SSM (Synchronous Status Messages) parameters can be configured on 7210 SAS-M and 7210 SAS-X shelves or ports, respectively.	See Procedures 19-5 and 20-1 for more information.
BFD on static routes	BFD can be enabled for static routes on a 7210 SAS-M or a 7210 SAS-X.	See Procedure 30-20 for more information.
PW standby signalling	PW standby signalling can be enabled for a VLL Epipe service on a 7210 SAS-M or a 7210 SAS-X.	See Procedure 70-1 for more information.
7210 SAS-X enhancements		
Egress Scheduler Mode	The Egress Scheduler Mode and Aggregate Rate Limit parameters can be configured on the access ports of a 7210 SAS-X, or a SAP, respectively.	See the *5620 SAM Parameter Guide* for more information.

(2 of 5)

Feature or function	Description	Reference for more information
7450 ESS and 7750 SR enhancements		
IEEE 1588 PTP clock	IEEE 1588 PTP clock support in 7450 ESS and 7750 SR Release 9.0 R4.	See Procedure 19-10 for more information.
IEEE 1588 PTP peer	IEEE 1588 PTP peer support in 7450 ESS and 7750 SR Release 9.0 R4.	See Procedure 19-11 for more information.
7705 SAR enhancements		
BITS clock on 7705 SAR 18	The 7705 SAR 18 supports the BITS timing reference. Supported in 7705 SAR Release 4.0 R2.	See chapter 19 for more information.
Standby Signaling Slave	Support for the Enable PW Standby Signaling Slave parameter on VLL Epipe, Cpipe, Ipipe, and Apipe endpoints. Supported in 7705 SAR Release 4.0 R2.	See chapter 70 for more information.
SAA Accounting Files	Support for the configuration of SAA accounting files for the collection of results from the CFM Loopback, CFM Link Trace, and CFM Two Way Delay tests. Supported in 7705 SAR Release 4.0 R2.	See chapter 78 for more information.
BFD for T-LDP	BFD Enabled parameter support on LDP peers in 7705 SAR Release 4.0 R3.	See chapter 31 for more information.
IEEE 1588 PTP clock	IEEE 1588 PTP clock support in 7705 SAR Release 4.0 R3.	See chapter 19 for more information.
OSPFv3	OSPFv3 protocol support in 7705 SAR Release 4.0 R4.	See chapter 31 for more information.
IPv6 BFD support	IPv6 BFD on network interfaces and IES L3 access interfaces. Supported in 7705 SAR Release 4.0 R3.	See chapters 30 and 73 for more information.
Device discovery and management over IPv6	Support for discovery and management of 7705 SAR NEs over IPv6. Supported in 7705 SAR Release 4.0 R1.	See chapters 13 and 14 for more information about device discovery and management using IPv6.
STP with VPLS	Support for STP on VPLS services. Supported in 7705 SAR Release 4.0 R4, consistent with the 7750 SR, 7450 ESS, and 7710 SR Release 7.0.	See chapter 71 for more information.
Multiple E1 multi-frames in single PW	The Payload Size parameter is configurable for a CEM SAP on a Cpipe service for VC type CESoPSN-CAS. Supported in 7705 SAR Release 4.0 R4 on the following hardware: • 16-port T1/E1 ASAP V1 and V2 adapter card • 32-port T1/E1 ASAP V2 adapter card • 7705 SAR-F	See chapter 70 for more information.
OmniSwitch enhancements		
Secure FTP client support for OS devices	The 5620 SAM supports secure and non-secure file transfers for backups, restores, software upgrades, and statistics collection. Secure file transfers using SSH2 is supported by all OS devices. The device mediation policy determines whether FTP or SCP is used during file transfers.	See chapter 14 for more information about configuring SSH2 on OS devices.
OS 6250M (Metro) device SLA testing	The 5620 SAM CPE SLA Test Head function allows you to perform a CPE SLA test using a CPE test-head profile or a group of profile on OS 6250M (Metro) devices. You can also run several tests on a CPE test-head profile or a group of profiles.	See chapter 78 for more information.
OS9-GNI-P24E Network Interface card support	The 5620 SAM supports the OS9-GNI-P24E Network Interface card on the OS 9700E and OS 9800E NEs.	See chapter 12 for more information.

(3 of 5)

Feature or function	Description	Reference for more information
Network management enhancements		
Dual Stack Lite address	A DS Lite address can be added when configuring NAT on a routing instance.	See Procedure 30-22 for more information.
IPCP subnet negotiation	A subnet can be assigned to a PPP host through the local user database by configuring the IPCP Subnet Negotiation or IP Address Prefix Length parameters when appropriate.	See Procedures 31-30, 68-3, and 68-32 for more information.
LI NAT sources configuration	LI NAT sources can be configured from the properties form of a mirror service.	See Procedure 34-9 for more information.
Protocol enhancements		
Multiple OSPF area IP interfaces	Support for multiple OSPF area IP interfaces extended to OSPFv3 areas on the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 31 for more information.
IGMP source and statistics viewing	The source of an IGMP group interface SAP group, as well as the statistics for an IGMP group interface SAP, can be viewed from the properties form of an applicable service.	See Procedure 31-42 for more information.
Policy enhancements		
Override policy aggregation	For policy types that allow multiple overrides to be configured, the Override Policy Items tab on the 5620 SAM GUI allows you to aggregate all subordinate override policies.	See chapter 46 for more information.
Connection profile policy	A connection profile is a list of VPI and VCI pairs that is supported on the 7750 SR-7, 7750 SR-12, 7750 SR-c12, 7750 SR-c4, 7450 ESS-7, and 7450 ESS-12. A connection profile SAP can be used to associate the ATM channel with a connection profile policy.	See chapter 57 for more information.
Policer mapping to local queue	Traffic flowing through a policer can now be directed to subsequently flow through an access egress queue.	See Procedure 47-3 for more information.
Percentage-based bandwidth in QoS policies	PIR and CIR shaping rates can now be specified as a percentage of available bandwidth for QoS ingress and egress queues, policers, and SAP overrides.	See Procedures 47-1, 47-3, and 47-44 for more information.
MSS for Hpol	The Aggregation Scheduler now supports the ability to add an ingress and egress policer control policy to further enhance rate limiting. This can only applied to an IOM3 port.	See Procedure 47-29 for more information.
ACL filter re-ordering confirmation	When defining the order in which an ACL IP filter policy tries to match filter ID entries with packets, a confirmation pop-up is invoked before the change is applied.	See Procedure 48-1 for more information.
HSMDA configurable Burst Thresholds	The 5620 SAM now supports specifying an explicit shaping burst size for an HSMDAv2.	See Procedures 19-24, 20-1, 47-3, and 47-12 for more information.
QoS and ACL MAC filtering based on VLAN ID	The 5620 SAM now allows SAPs to perform QoS and MAC filtering based on the VLAN ID field. This feature is applicable to VPLS, I-VPLS, MVPLS, and Epipe SAPs configured on IMM and IOM3 hardware.	See Procedures 48-3 and 47-1 for more information.
Routing policy enhancements	When configuring a local routing policy statement, the interface index of the interface to which IGMP multicast traffic is to be redirected can be specified.	See Procedure 30-11 for more information.
Ingress multicast reporting destination policy creation and statistics viewing	An ingress multicast reporting destination policy can be created, and the related statistics for a particular NE can be viewed.	See Procedures 49-5 and 49-5 for more information.

(4 of 5)

Feature or function	Description	Reference for more information
Subscriber multicast CAC policy creation	A subscriber multicast CAC policy can be created.	See chapter 68 for more information.
Subscriber profile policy bindings	Both an IGMP policy and a subscriber multicast CAC policy can be bound to a subscriber profile.	See chapter 68 for more information.
PPP Idle Timeout	When creating or modifying an SLA profile, PPP Idle Timeout can be configured for a category.	See chapter 68 for more information.
IGMP policy enhancements	Additional parameters can be configured in the multicast reporting panel on the properties form of an IGMP policy. A redirection policy for filtering IGMP packets can be specified.	See chapter 68 for more information.
Service management enhancements		
Ethernet-CFM redundancy	You can configure Ethernet-CFM redundancy to link MEPs to the state of the resiliency mechanism that is supported in MC-LAGs.	See chapter 80 for more information.
Virtual port statistics	Virtual port statistics can now be displayed for all queues forwarding to a virtual port configured on the egress of an Ethernet port.	See chapter 66 for more information.
5620 SAM documentation enhancements		
Scope of command roles and permissions appendix	An appendix featuring tabular lists of the following information: • All assignable scope of command role permissions and descriptions of their functions. • All predefined scope of command roles and a list of permissions for each role.	See Appendix A for more information.
5620 SAM User Guide content reorganization	The Introduction volume of the *5620 SAM User Guide* has been reorganized and now includes a detailed description of the 5620 SAM GUI and its components, such as configuration forms, the navigation tree, contextual menus, maps, and the equipment window.	See chapters 3, 4, 5, and * for more information. Note: The equipment window chapter was removed in 90R5.
5620 SAM Troubleshooting Guide reorganization	The 5620 SAM alarm description tables are now in an appendix of this guide.	See the *5620 SAM Troubleshooting Guide*.

(5 of 5)

2.6 5620 SAM Release 9.0 R2

5620 SAM Release 9.0 R2 is a maintenance release. No features have been added.

2.7 5620 SAM Release 9.0 R1

Table 2-4 lists the features and functions added in 5620 SAM Release 9.0 R1.

Table 2-4 5620 SAM Release 9.0 R1 features

Feature or function	Description	Reference for more information
GUI enhancements		
Configuration form enhancements	The 5620 SAM client GUI configuration form enhancements include: • collapsible panels to improve navigability of configuration forms • asterisks on configuration form tab button and panel labels to indicate that information is missing or incorrect • a search capability that allows you to locate specific attributes on a configuration form • the navigation tree is now on the left side of service and network element configuration forms, for improved object accessibility • the ability to lock tabs on a configuration form, which allows you to open multiple tabs on a configuration form at the same time • the ability to undock configurable object forms from the main configuration form window • a tool tip displays a descriptive label for service and network element configuration forms • an icon that denotes a change on a configuration form tab and helps the user navigate to the location of the change • specification of the columns to display in a list • improved the ability to customize the sequence in which columns in a list appear	See sections 3.1 and 3.2 for more information. See Procedure 3-33 for more information about viewing and managing listed information.
Map enhancements		
Hidden upper-layer adjacency links	The 5620 SAM Physical Topology Map view highlights physical links carrying hidden links. The Highlight Upper Layer Adjacency Links contextual menu command displays the hidden adjacencies.	See chapter 5 for more information.
Map endpoint enhancement	The Service Topology Map view adds a new Endpoint Layout option to the Auto-Layout tool for VPLS, VLL, mirror, and composite services.	See chapter 5 for more information.
5620 SAM System management enhancements		
Changes to Microsoft Windows support	The installation or upgrade of a 5620 SAM database or main server is no longer supported on a Microsoft Windows platform. 5620 SAM support for Windows is limited to single-user client installation and upgrade only.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about 5620 SAM system migration from Microsoft Windows to Solaris.
Security management	Security enhancements to the 5620 SAM allow system administrators to manage client GUI user security more effectively. System administrators can use security management to request a password change for 5620 SAM users	See chapter 9 for more information.
Automatic database reinstantiation	The 5620 SAM supports automatic reinstantiation of the primary database in the event of a database failover.	See chapter 7 for more information.
New Oracle version	The 5620 SAM, Release 9.0, uses Oracle version 11r2 as the RDBMS.	See the *5620 SAM Planning Guide* and *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

(1 of 12)

Feature or function	Description	Reference for more information
System component configuration	If an IP address change is required for one or more of the 5620 SAM workstations in the following scenarios, please contact your Alcatel-Lucent technical support representative: • when the station in a collocated standalone 5620 SAM system requires a different IP address • when a new IP address is required by the primary or standby station, or both stations, in a collocated redundant 5620 SAM system • when a new IP address is required by any or all of the primary or standby stations, in a distributed redundant 5620 SAM system	See chapter 6 for more information.
Device management enhancements		
Automated SSL configuration	You can configure SSL on 5620 SAM components using the 5620 SAM installation and configuration utility; no manual configuration is required. After you configure SSL on a Release 9.0 5620 SAM system, the 5620 SAM preserves the SSL configuration through subsequent upgrades.	See chapter 10 and the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
EMS configuration	The 5620 SAM supports the discovery and monitoring of Element Manager Systems.	See chapter 14 for more information.
Object life cycle state configuration extended	The ability to configure the object life cycle state has been extended to include SAPs (L2 access interfaces and L3 access interfaces) on VLL, VPLS, VPRN, MVPLS, and IES services.	See chapter 28 for information about setting the OLC state.
ISA-NAT member usage stats	The 5620 SAM supports the collection of ISA-NAT member usage statistics.	See chapter 18 for more information.
Signal capability	The 5620 SAM supports enabling a Signal Capability parameter to specify whether or not a Local PE should signal its Hash label capability to a remote PE.	See chapter 14 in the *5620 SAM Parameter Guide* for more information.
HSMDAv2 daughter card	Version 2 of the HSMDA daughter is introduced in this release. Numerous portions of the *5620 SAM User Guide* have been added or modified to address the capabilities of the new card, including: • QoS - Egress HSMDA scheduling • QoS - Egress HSMDA scheduling overrides • HSMDA WRR Policy • HSMDA QoS Pool modifications • HSMDA Egress secondary shapers • HSMDA LAGs and LAG Groups • Network queue policies • QoS policy overrides on L2/L3 access interfaces • Subscriber profiles • 7750 SR and 7450 ESS support • Ethernet ports • VPLS/MVPLS services • VLL Epipe services • IES services • VPRN services	See the following *5620 SAM User Guide* chapters and related *5620 SAM Parameter Guide* chapters for more information: • chapter 47 • chapters 20 and 47 • chapter 47 • chapter 20 • chapter 20 • chapter 18 • chapter 47 • chapter 47 • chapter 68 • chapter 19 • chapter 20 • chapter 71 • chapter 70 • chapter 73 • chapter 74
TWAMP server support	The 5620 SAM supports configuration of TWAMP servers.	See chapter 17 for more information.

(2 of 12)

Feature or function	Description	Reference for more information
Soft reset support	Soft reset support is extended to include the following: • 1-port 100GE CFP IMM • 12-port 10GE SF IMM • 10Gig-base Extended Performance MDAs that are in XGig WAN mode	See Procedure 23-12 for more information.
1830 PSS enhancements		
—	See the *5620 SAM Optical User Guide* for information about features and functions that are specific to optical device support.	—
7210 SAS-D enhancements		
Silo and discovery, and equipment support	The following functions are extended to include the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR: • Silo and discovery • Card support • Port support • LAG • In-band management • Backup and Restore There is no fan tray support for the 7210 SAS-D.	See chapters 12, 13, 16, and 23 for more information.
Dying Gasp alarm	The Dying Gasp alarm supported is extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR. The Dying Gasp alarm is triggered by a trap from the 7210 SAS when a 7450 ESS goes out of service.	See the *5620 SAM Troubleshooting Guide* for more information.
IES Q1.Q2 parameter configuration	Configuration of the Q1.Q2Q parameter is extended to the 7210 SAS-D. The Q1.Q2 parameter is configurable when the port Encap Type parameter is set to Q1.Q2. The range of values are configurable only on the Outer Encapsulation parameter.	See the *5620 SAM Parameter Guide* for more information on the IES Outer encapsulation parameter.
VPLS and MVPLS	VPLS and MVPLS support is extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapter 71 for more information.
VLL Epipe and LLF support	VLL Epipe configuration and LLF in VLL Epipe services capabilities are extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapter 70 for more information.
Mirror services	Mirror services support is extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapter 72 for more information.
Static routes	The configuration of static routes is extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapter 30 for more information.
H-Metering	The configuration of H-Metering is extended to the 7210 SAS-D 6F 4T.	See Procedures 70-13 and 71-3 for more information.
Q in Q Ethertype	The configuration of Q in Q Ethertype is extended to include the 7210 SAS-D. The Q in Q Ethertype parameter is configurable when the port Encap Type parameter is set to Q in Q.	See Procedure 20-1 for more information.
ACL IP and ACL MAC filter policies	The configuration of ACL IP Filter policies and ACL MAC Filter policies are extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapters 48 and 50 for more information on Filter policies.
Accounting and Performance statistics	Support for Accounting and Performance statistics is extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See the *5620 SAM Statistics Management Guide* for more information.

(3 of 12)

Feature or function	Description	Reference for more information
QoS policies	The following QoS policy capabilities have been extended to the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR: • 7210 Port Access Egress • 7210 Access Ingress • 7210 Network: Supports only Port types for the Network policy. Forwarding classes: only Dot1p In Profile and Dot1p Out Profile for Egress and Ingress Dot1p. Multi-Point: true only. 12 Meters are supported. Mode: srTCM and trTCM. Not supported: DSCP and LSP. • 7210 Network Queue: Not supported: Queue Management Policy and Port Parent in the NQueueEntry, 7210 Network Queue, Global Policy [Create] form. • 7210 Slope • 7210 Port Scheduler	See chapters 12 and 47 for more information.
Licensing	You can manage or unmanage SAS-D NEs on the 5620 SAM server based on the licenses. You can view license details and remaining licenses on the 5620 SAM GUI.	See chapter 6 for more information.
Ethernet OAM	802.1ag supports only CFM loopback and CFM link trace on the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR.	See chapters 38 and 80 and for more information.
7210 SAS-E enhancements		
dot1q NULL SAP	The 5620 SAM supports dot1q NULL SAP on the 7210 SAS-E.	See the *5620 SAM Parameter Guide* for more information.
Y.1731 Ethernet OAM	The 5620 SAM supports EthTest, One Way Delay, Two Way Delay on the 7210 SAS-E, Release 2.0 or later.	See chapter 38 for more information.
7210 SAS-M enhancements		
Dynamic reservation for non-customer traffic ports	Dynamic reservation for non-customer traffic ports is supported on 7210 SAS-M 24F 2XFP, and 7210 SAS-M 24F 2XFP [ETR], Release 3.0 R1.	See chapter 20 for more information.
H-Metering	H-Metering is supported on the 7210 SAS-M, Release 3.0 R1 and later.	See Procedures 70-13 and 71-3 for more information.
Q in Q Ethertype configuration	The Q in Q Ethertype parameter is configurable when the port Encap Type parameter is set to Q in Q for the 7210 SAS-M, Release 3.0 R1 and later.	See Procedure 20-1 for more information.
VCCV trace test for Cpipe and Epipe	VCCV trace test for Cpipe and Epipe is supported on the 7210 SAS-M, Release 2.0R5, and Release 3.0 R1 and later.	See chapters 38 and 70 for more information.
BFD support	BFD is supported on the RSVP interface for 7210 SAS-M, Release 3.01 R1 and later.	See chapters 30, 31, and 74 for more information.
MSTP	You can run individual STPs for every VLAN for the 7210 SAS-M, Release 3.01 R1 and later.	See chapter 33 for more information.
L2 Access Uplink support	The 5620 SAM supports: • 2x10GigE XFP MDA for L2 Access uplink and access port modes. Access encapsulation types supported are Null, dot1q and Q in Q. • Access Mode supports Null, Q in Q and dot1q. Q in Q Ethertype attribute in 7210 SAS-M Uplink is applicable to the Ports which support uplink mode or Access Q in Q Encap.This attribute is not applicable when the Mode is Access and the encap type is either Null or dot1q.	See chapter 20 for more information.
Mirror Service	Mirror Service has been extended to include local mirroring, destination sites, and one L2 Access interface.	See chapter 72 for more information.

(4 of 12)

Feature or function	Description	Reference for more information
Backup and restore	The backup and restore functionality has been extended to include the 7210 SAS-M.	See chapter 23 to create a device backup and restore policy.
Software upgrade	The software upgrade functionality has been extended to include the 7210 SAS-M.	See Procedure 23-11 to create a Software upgrade policy.
Statistics management	Statistics management for the 7210 SAS-M has been extended to include: • Accounting and Performance statistics • ICMP Ping and ICMP Trace for management ports	See the *5620 SAM Statistics Management Guide* for more information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM.
Y.1731 Ethernet OAM tests and the 802.1ag support.	Ethernet OAM functionality (CFM continuity check, CFM loopback, EthTest, CFM link trace, CFM one way delay, and CFM two way delay tests) on Y.1731 platform and on 802.1ag only CFM loopback and CFM link trace is supported on 7210 SAS-M uplink NEs.	See chapters 38 and 80 for more information.
IES support	IES support is extended to 7210 SAS-M uplink NEs in access mode.	See Procedure 73-1 for more information.
Static routes	Static route support is extended to 7210 SAS-M.	See chapter 30 for more information.
VPLS and VLL	VPLS and VLL services are extended to VLAN uplink.	See chapter 71 for more information.
Link Loss Forwarding	The 5620 SAM supports link loss forwarding (LLF) functions for the 7210 SAS-M and 7210 SAS-M24F2X NEs in VLL Epipe services.	See Procedure 70-13 for more information.
QoS Policies	The 7210 SAS-M now supports the following QoS Policies: • 7210 Access Ingress • 7210 Port Access Egress • 7210 Network • 7210 Network Queue • 7210 Slope • 7210 Port Scheduler	See chapter 47 for more information.
7210 SAS -X enhancements		
Out-of-band management	Out-of-band management support is extended to the 7210 SAS-X 24F 2XFP	See chapter 13 for more information.
Ethernet Ring Protection (G.8032)	The 5620 SAM supports Ethernet Ring Protection (G.8032) on the 7210 SAS 3.0, Release 1 and later devices with one exception. Ethernet Ring Protection is not supported on the 7210 SAS-X 24F 2XFP, Release 3.0 R1. It is supported on 7210 SAS-X 24F 2XFP, Release 3.0 R2 Ethernet ring protection is provided by RPLs employed to protect the ring and help achieve high reliability and network stability.	See chapter 12 and Procedures 33-7 and 33-10 for more information.
Aggregate Rate Limit	The Aggregate Rate Limit parameter support is extended to the port level and the SAP level for access ports on the 7210 SAS-X Release 2.0 R7 port Ethernet daughter card.	See Procedures 17-18, 70-13, 71-3 for more information.
IGMP snooping	IGMP snooping support is extended to the 7210 SAS-X 24F 2XFP Release 3.0 R2 or later.	See chapter 71 and Procedure 71-3 for more information.
VCCV trace test support for Epipe	The VCCV trace test for Epipe functionality is extended to Release 2.0 R5, and Release 3.0 R1 and later.	See chapters 38 and 70 for more information.

(5 of 12)

Feature or function	Description	Reference for more information
BFD support on the RSVP interface.	BFD support on the RSVP interface is extended to include the 7210 SAS-X 24F 2XFP.	See chapters 30, 31, and 74.
MSTP	You can run individual STPs for every VLAN for the 7210 SAS-X 24F 2XFP.	See chapter 33 for more information.
7450 ESS, 7750 SR, and 7710 SR enhancements		
Support for new hardware	The 5620 SAM supports the use of VSM-CCA-XP daughter cards on the 7750 SR and 7450 ESS.	See chapter 19 for more information.
CES MDA support on 7450 ESS in mixed mode	The 5620 SAM supports the CES MDA cards on the 7450 ESS when this unit is configured for mixed mode operation, irrespective of chassis mode.	See chapter 19 for more information about daughter card support. See Procedures 19-1 and 19-4 for more information on chassis modes and enabling mixed mode operation.
LAG active/standby operation without LACP	The 5620 SAM supports configuration of the Standby Signalling parameter in the LACP configuration on LAG member links on the 7750 SR and 7450 ESS.	See chapter 18 for more information.
Scale to 100G IPsec	The 5620 SAM supports a range of 1 to 16 for the Group Number parameter on ISA-IPsec groups on the 7750 SR and 7450 ESS, Release 9.0 R1 and later.	See chapter 18 for more information.
Hash label support for chassis mode B	The 5620 SAM supports Hash labels on SDP bindings for 7750 SR NEs in chassis mode B.	See chapter 14 in the *5620 SAM Parameter Guide* for more information.
Multiple OSPF area IP interfaces	The 5620 SAM supports the configuration of IP interfaces that can belong to multiple OSPFv2 areas on the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 31 for more information.
IPsec IKE	The 5620 SAM supports a range of 0 to 64 characters for the Pre Shared Key parameter on an IPsec tunnel or IPsec gateway on the 7750 SR and 7450 ESS Release 9.0 R1 and later.	See chapter 35 for more information.
GRE termination in VPRN	The 5620 SAM supports the configuration of a GRE tunnel termination on a VPRN site IPsec interface on the 7750 SR, Release 8.0 R5 and later.	See chapter 35 for more information.
Support for Local DHCPv6 Servers	The 5620 SAM supports the configuration of Local DHCPv6 Servers on the 7750 SR and on the 7450 ESS in mixed mode.	See Procedures 30-2 and 74-1 for more information.
IGMP reporting of join, leave, and expiry events	The 5620 SAM supports the ability to generate reports and view statistics related to IGMP multicast traffic. This feature is supported on the 7750 SR and 7450 ESS (mixed mode), Release 9.0 R3 or later.	See Procedures 30-2, 31-41, 49-5, and 68-9 for more information.

(6 of 12)

Feature or function	Description	Reference for more information

IPv6 support on 7750 SR-7 and 7750 SR-12 in chassis modes A and B	The configuration of IPv6 addressing on network ports of 7750 SR-7 and 7750 SR-12 devices operating in chassis mode A or B is introduced in this release. Mixed mode must be enabled and this functionality is only applicable to units running an IOM3-XP or IMM. IPv6 can be configured on:
	• Network interfaces
	• OSPFv3 instances
	• IS-IS instances
	• Route aggregations
	• Source IP addresses
	• IGMP instances
	• MLD instances
	• RIP instances
	• BGP instances
	• routing policies
	• static routes
	• ACL IPv6 Filter policies
	• access ingress policies
	• VRRP policies
	• MAF and CPM filters
	• ISA-IPSEC groups
	• VLL SAPs
	• IES interfaces as follows:
	  • access interfaces
	  • subscriber interfaces
	  • IPSec interfaces
	• VPRN service interfaces as follows:
	  • access interfaces
	  • IPSec interfaces
		See chapter 18 for more information on card provisioning and ISA-IPSEC groups.
		See chapter 18 and Procedures 19-1 and 19-4 for more information on chassis modes and enabling mixed mode operation and ISA-IPSEC groups.
		See chapter 21 for more information on MAF and CPM filters.
		See chapter 30 for more information on routing policies.
		See chapter 31 for more information on protocol configuration.
		See chapter 47 for more information on access ingress policies.
		See chapter 48 for more information on ACL IPv6 filter policies.
		See chapter 51 for more information on VRRP policies.
		See chapter 70 for more information on VLL service configuration.
		See chapter 73 for more information on IES configuration.
		See chapter 74 for more information on VPRN service configuration.

IPVPN service label per next-hop operation	The 5620 SAM supports the Label Mode parameter on VPRN sites on the 7750 SR and 7450 ESS.	See chapter 74 for more information.
FIB prioritization per VPRN operation	The 5620 SAM supports the FIB Priority parameter on VPRN sites on the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 74 for more information.
BGP flowspec support on 7750 SR and 7450 ESS	The 5620 SAM supports configuration of the Flowspec Validate parameter on global, peer group, and peer level BGP sites, network interfaces, IES L3 access interfaces, and IES spoke SDP bindings.	See chapters 30, 31, and 73 for more information.
VLL Cpipe support extended to 7450 ESS and 7750 SR-1	The 5620 SAM supports the creation of a VLL Cpipe on the 7450 ESS-12 and 7450 ESS-7 in mixed mode or non-mixed mode, Release 8.0 R5 or later, and on the 7450 ESS-1, 7450 ESS-6 and 7750 SR-1, Release 8.0 R6 or later.	See Procedure 70-9 for more information.
Carrier serving carrier VPRN	The 5620 SAM supports network interface configuration on a VPRN service on the 7750 SR and 7450 ESS, Release 9.0 R1 and later.	See chapter 74 for more information.
7450 ESS support	• The Dying Gasp alarm is triggered by a trap from the 7450 ESS node when a 7210 SAS go down.	See the *5620 SAM Troubleshooting Guide* for more information on Dying Gasp alarm.
7705 SAR enhancements		

(7 of 12)

Feature or function	Description	Reference for more information
7705 SAR-18 support	The 5620 SAM supports the 7705 SAR-18 hardware platform. The 7705 SAR-18 chassis is functionally identical to the 7705 SAR-8, with the following differences: • 16 daughter card slots. (For, Release 9.0 R1, 12 of these card slots are configurable from the 5620 SAM. The remaining 4 slots are reserved.) • BITS timing interface. • No external timing interface.	See chapter 19 for more information.
802.1 PAE support on 7705 SAR	The 5620 SAM supports IEEE 802.1 PAE on the 7705 SAR, Release 4.0 R1 and later. This support is consistent with the 7750 SR, Release 7.0	See chapter 19 for more information.
CFM Loopback on 7705 SAR	The 5620 SAM supports CFM LoopBack Mode configuration on Ethernet ports on the 7705 SAR, Release 4.0 R1.	See chapter 20 for more information.
Swap MAC Address on 7705 SAR	The 5620 SAM supports Swap MAC Address configuration on Ethernet ports on the 7705 SAR, Release 4.0 R1.	See chapter 20 for more information.
16 port T1/E1 ASAP MDA on 7705 SAR	The 5620 SAM supports the 16 port T1/E1 ASAP daughter card on the 7705 SAR, Release 4.0 R3.	See chapter 19 for more information.
32 port T1/E1 adapter card on 7705 SAR	The 5620 SAM supports the 32 port T1/E1 ASAP adapter card on the 7705 SAR, Release 4.0 R3.	See chapter 19 for more information.
Graceful shutdown support on 7705 SAR 4.0 R1	The 5620 SAM supports the Graceful Shutdown parameters for RSVP sites and interfaces on the 7705 SAR, Release 4.0 R1 or later.	See chapter 31 for more information.
Ethernet OAM thresholds on 7705 SAR 4.0 R1	The 5620 SAM supports the ETH test and One Way Delay test thresholds on the 7705 SAR 4.0 R1, consistent with Release 7.0 of the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 38 for more information.
OAM ping and trace results on 7705 SAR 4.0 R1	The 5620 SAM supports the reporting of test result status on the 7705 SAR 4.0 R1, consistent with Release 7.0 R3 of the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 38 for more information.
Routing policy enhancements	The 5620 SAM supports the No Route Tag parameter on routing policy statements on the 7705 SAR 4.0 R1.	See chapter 30 for more information.
BGP enhancements on 7705 SAR 4.0 R1	The 5620 SAM supports the Local AS, Peer AS, Hold Time, and Remove Private AS parameters on the 7705 SAR, Release 4.0 R1 or later.	See chapters 31 and 68 for more information.
Filter policy support on 7705 SAR 4.0 R1	The 5620 SAM supports ACL IPv6 Filter policies, ACL MAC Filter policies, and CPM IPv6 Filter policies on the 7705 SAR, Release 4.0 R1 or later. Partial distribution of ACL IPv6, ACL MAC, or CPM IPv6 filters is not supported. Each entry, property, and value within a given filter policy must be supported by the target 7705 SAR NE.	See chapter 48 for more information.
Fabric Profile policy enhancement on 7705 SAR 4.0 R1	The 5620 SAM supports the Multipoint Rate parameter in 7705 SAR Fabric Profile policies on the 7705 SAR, Release 4.0 R1 or later.	See chapter 47 for more information.
Access ingress policy enhancements on 7705 SAR 4.0 R1	The 5620 SAM supports the Multipoint Queue ID, Broadcast Queue ID, and Unknown Queue ID forwarding class parameters on the 7705 SAR 4.0 R1.	See chapter 47 for more information.
Network queue policy enhancements on 7705 SAR 4.0 R1	The 5620 SAM supports multicast network queues 9 through 16 and the Multicast Queue ID forwarding class parameter on the 7705 SAR 4.0 R1.	See chapter 47 for more information.

(8 of 12)

Feature or function	Description	Reference for more information
Spoke SDP termination for IES and VPRN services on 7705 SAR 4.0 R2	The 5620 SAM supports spoke SDP terminations for IES and VPRN services on the 7705 SAR, Release 4.0 R2 or later.	See chapters 73 and 74 for more information.
9500 MPR enhancements		
9500 MPR port segregation	The 5620 SAM supports the configuration of port segregation on the 9500 MPR using a wizard.	See chapter 20 for more information.
9500 MPR timing synchronization	The 5620 SAM supports timing synchronization on 9500 MPR NEs.	See chapter 19 for more information.
9500 MPR release support	The 5620 SAM provides silo and discovery support for the following ETSI and ANSI releases: • 9500 MPR ETSI: Release 2.1 • 9500 MPR ANSI: Release 2.2.0 • 9500 MPR ETSI and ANSI: Release 3.0.0 GNE support: • 9400 AWY, MPR-SA, MPR-E, MSS-1C The 5620 SAM does not provide support for the following ETSI and ANSI releases: • 9500 MPR ETSI: Release 1.2 and Release 1.3 • 9500 MPR ANSI: Release 2.1	—
9500 MPR dot1q VLAN services support	The 5620 SAM supports the creation of dot1q VLAN services on both the MSS-4 and MSS-8 variants of the 9500 MPR (ANSI), release 3.0 or later.	See Procedure 69-8 for more information.
9500 MPR Path Management support	The 5620 SAM supports redundant protection paths provided by the radio system for the MPR family. Path Management for protected link 1 x (1+1).	See chapters 5 and 70 for more information.
9500 MPR Extended Backhaul service	The 5620 SAM supports: • SAP/XC (Physical Link) completion • Termination points (TP) related to transport service SAP and book ending equipment ports.	See Procedure 70-3 for more information.
9500 MPR card support	The 5620 SAM supports: • The MPT-ACC card is supported on 9500 MPR for ANSI Release 3.0.0. • The 2 x STM card is supported on 9500 MPR for ETSI Release 3.0.0. • Services over SDH ports (SDH to SDH) on 9500 MPR Cpipe for ETSI Release 3.0.0	See chapters 12, 19, and 70 for more information.
5620 SAM LTE ePC enhancements		
—	See the *5620 SAM LTE ePC User Guide* for information about LTE ePC features and functions.	—
5620 SAM LTE RAN enhancements		
—	See the *5620 SAM LTE RAN User Guide* for information about LTE RAN features and functions.	—
OmniSwitch enhancements		

(9 of 12)

Feature or function	Description	Reference for more information

OmniSwitch support	The 5620 SAM supports:
	• AOS Release 6.4.4 support on OS 6400, OS 6850, OS 6850E, OS 6855, OS 9700E, and OS 9800E NEs.
	• PIM and RIP routing protocol, and OSPF for the default routing instance on OS 6850, OS 6850E, and OS 6855, Release 6.4.4 or later.
	• RIP routing protocol on OS 6400, Release 6.4.4 or later.
	• OSPF, PIM, and RIP on VRF instances supported on OS 6855 U24X, Release 6.4.4 or later.
	• G8032 Ethernet ring protection for OS 6400, OS 6850, OS 6850E, OS 6855, OS 9700E, and OS 9800E, Release 6.4.4 or later, and OS 6250 (Metro) NEs, Release 6.6.2 or later. Note: For OmniSwitch NEs, only Ethernet ring element (and not Ethernet ring) is supported.
	  • EPS path configuration
	  • EPS service configuration (Standard and Stacked VLAN)
	  • protected service configuration
	  • statistics collection
	  • alarm support (automatic alarm clearing is not supported)
	  • EPS OAM
	• OS 6850E support for Release 6.4.4 or later:
	  • software upgrade and backup/restore
	  • licensing support
	• LAG OAM support for OS Releases 6.4.4 or later, and 6.6.2 or later
		See chapter 12 for more information.
		See chapters 16, 126, 167, 182, and 184 for more information.
		See Procedure 33-8 for more information.
		See chapters 37 and 78 for more information.
		See chapter 38 (Ethernet CFM) for more information.
		See Procedures 23-8, 23-9, and 23-16 for more information.
		See chapter 6 for more information.
		See Procedure 19-22 for more information.
		See chapters 69, 31, 38, 47, 56 for more information.
		See chapter 38 for more information.

Network management enhancements		
Synchronization of static port forwards	The 5620 SAM supports the synchronization of static port forwards.	See chapters 30, 68, and 74 for more information.
NAT enhancements	The 5620 SAM supports the configuration of many new parameters on the NAT configuration and NAT pool forms.	See chapters 30, 68, and 74 for more information.
IPv6 BFD support	The 5620 SAM supports IPv6 BFD on network interfaces, IES and VPRN L3 access interfaces, OSPFv3 interfaces, network and IES PIM interfaces, IS-IS interfaces, and on VRRP instances.	See chapters 30, 31, 39, 73, and 74 for more information.
MC APS enhancements	Bidirectional MC APS support is extended to include all non-channelized SONET/SDH MDAs and CMAs.	See chapter 40 for more information.
G.8032 multi-ring support	The 5620 SAM supports service tunnel Ethernet sub-ring functionality.	See chapter 33 for more information.
BGP best external	The 5620 SAM supports the advertisement of best external routes by a BGP site to its internal BGP peers.	See chapter 31 for more information.
Path MTU discovery in BGP	The 5620 SAM supports path MTU discovery for global BGP, BGP group, BGP peers, and LDP peers on virtual routers and VPRN routing instances.	See chapter 31 for more information.
PIM ECMP Hash label support	The 5620 SAM supports ECMP Hash labels on PIM sites.	See chapter 31 for more information.
mLDP in mVPN	The 5620 SAM supports mLDP inclusive tunnels in mVPN.	See chapter 31 for more information.
Exponential backoff timer	The 5620 SAM supports an Exponential backoff timer for MPLS LSPs.	See chapter 32 for more information.

(10 of 12)

Feature or function	Description	Reference for more information
CFM SLM test	The 5620 SAM supports a two-way CFM Synthetic Loss Measurement OAM diagnostic test.	See chapter 38 for more information.
Protocol enhancements		
—	—	—
Policy enhancements		
ISID level shaping on B-SAP	The 5620 SAM supports the Packet Byte Offset parameter on egress queues on IOM3-XP cards.	See chapter 47 for more information.
RADIUS-based accounting enhancements	You can use a 5620 SAM RADIUS-based accounting policy to collect per-host accounting statistics on Release 9.0 and later NEs.	See chapter 53 for more information.
Additional origin types for BGP routes	The 5620 SAM allows the selection of additional origin types for BGP routes to be considered as match criteria for routing policy statements.	See the *5620 SAM Parameter Guide* for more information on the Origin parameter.
Service management enhancements		
System preferences support for Services	The 5620 SAM supports the configuration of the system preferences of services that are associated with customers.	See chapter 67 for more information.
ESM enhancements	The 5620 SAM supports URPF check on subscriber interfaces for managed-route hosts. This feature supports Group Interfaces having the same functionality as IES and VPRN L3 Access Interfaces. Unicast RFP stats are collected for Group Interfaces.	See chapters 30, 73, and 74 for more information.
AA Customer level Apdex/MOS thresholds	The 5620 SAM supports a series of Apdex score thresholds on a per customer basis.	See Procedure 67-5 for more information.
AA transit IP policy	The 5620 SAM supports the configuration of AA transit IP policies.	See chapter 77 for more information.
Support for static port forwarding on residential subscriber instances	The 5620 SAM supports configuration of L2-Aware SPFs on residential subscriber instances.	See chapter 68 for more information.
LCP Keep Alive Interval	The 5620 SAM allows configuration of a new minimum value for the LCP Keep Alive Interval parameter.	See the *5620 SAM Parameter Guide* for more information.
PBB restrictions relaxed	Chassis mode restrictions for PBB Dual Homing and SAP-type restrictions for PBB Epipe local switching have been relaxed.	See chapter 71 for more information on VPLS and chapter 70 for more information on VLL Epipe.
MDT-SAFI supported on BGP and PIM sites	MDT-SAFI was added to the permitted Family and Address Family values on BGP sites and PIM sites.	See chapter 71 for more information on VPLS and chapter 74 for more information on VPRN.
Service size reduction	The 5620 SAM supports moving sites from one service to another of the same type in order to reduce the overall size of a particular service.	See chapter 67 for more information.
PW status signalling support	The 5620 SAM supports PW status signalling on spoke SDP bindings for VPLS and VLL Epipe services.	See chapter 71 for more information on VPLS and chapter 70 for more information on VLL.
Unnumbered subscriber interfaces	The 5620 SAM supports the configuration of unnumbered IES and VPRN subscriber interfaces.	See Procedures 73-7 and 74-12 for more information.

(11 of 12)

Feature or function	Description	Reference for more information
Operational groups	The 5620 SAM supports the creation of operational groups and the assignment of members and monitors to those groups.	See Procedures 17-3, 71-3, 71-5, and 71-6 for more information.
Block spoke SDP transmission on VLL Epipe	The 5620 SAM supports the Enable PW Standby Signaling Slave parameter on VLL Epipe endpoints and spoke SDP bindings.	See chapter 70 for more information.
Extended MEP support	The 5620 SAM supports the creation of facility MEPs on network interfaces, ports, and LAGs. The creation of virtual facility tunnel MEPs on LAG ports is also supported.	See chapter 80 for more information.
Router alert check configuration for IGMP	The 5620 SAM supports the Disable Router Alert Check parameter on certain IGMP interface objects.	See chapters 31, 71, 73, and 74 for more information.
Add or create services in composite service flat map view.	You can create a new service or add existing services or sites in the Composite Service Flat Topology Map view.	See chapter 76 for more information.
Additional features		
LogViewer enhancements	The 5620 SAM LogViewer utility includes the following: • Task Tracker, Web SSO, rsynch, and scheduler log support • improved performance • greater customization • user preference preservation across upgrades • multiple UI improvements	See the *5620 SAM Troubleshooting Guide* for more information.
Supervision Module	The 5620 SAM supports the launch of the 5620 SAM Supervision Module from a client GUI. This web-based application provides summarized views of objects monitored by the client GUI from which it is launched.	See the *5620 SAM Supervision Module User Guide* for more information.
Additional application filter expression types	The 5620 SAM allows the selection of TLS Certificate Subject Organization and TLS Certificate Subject Common as application filter expression types.	See the *5620 SAM Parameter Guide* for more information on the Application Filter Expression Type parameter.
5620 SAM documentation enhancements		
—	—	—
Discontinued support		
—	—	—

(12 of 12)

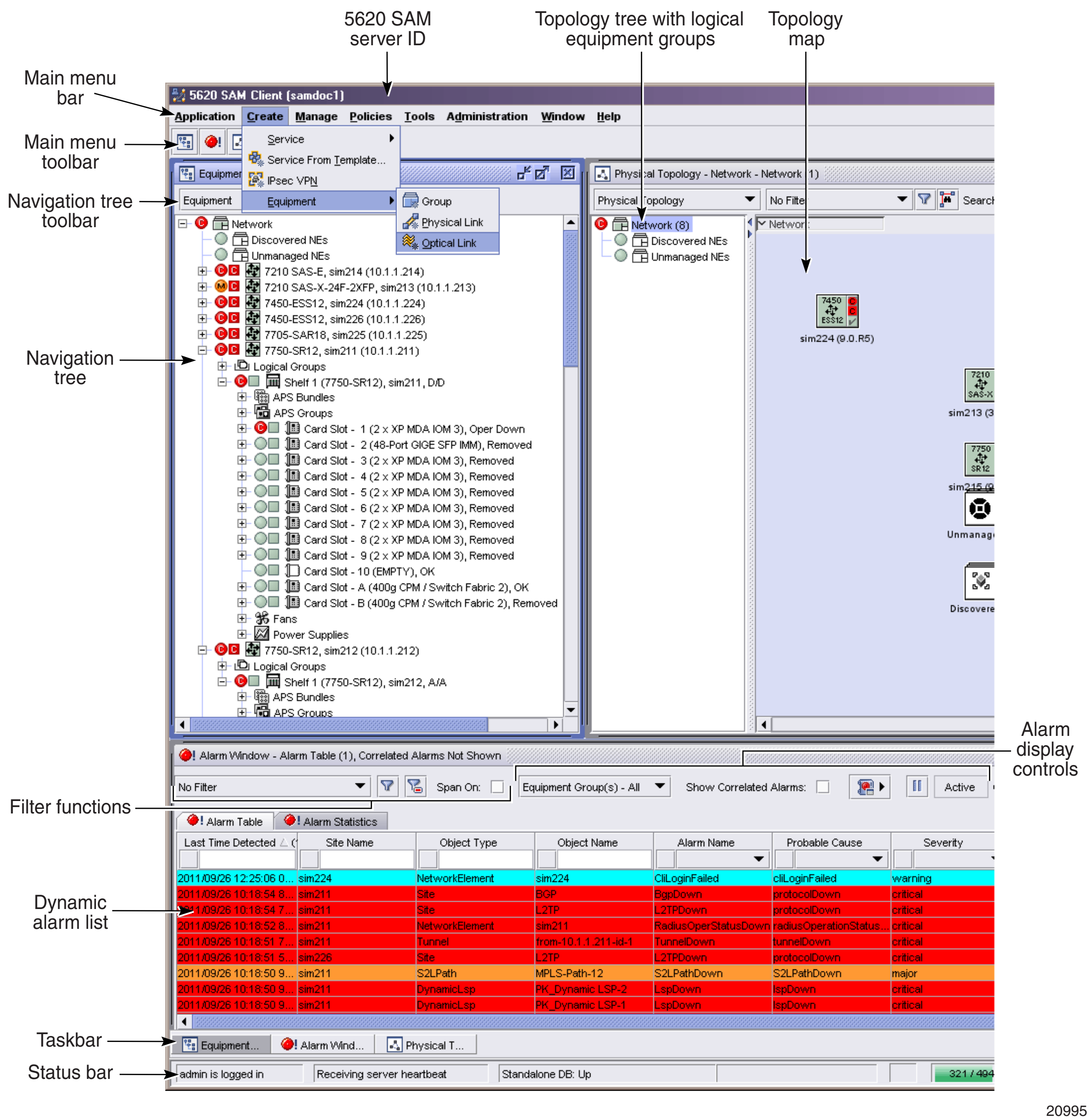
3 — 5620 SAM GUI overview

3.1 5620 SAM GUI overview

The 5620 SAM GUI is a graphical interface on a 5620 SAM client station that allows a NOC operator to perform network management functions. Multiple 5620 SAM GUI clients can connect to a 5620 SAM server.

The main GUI elements, as shown in Figure 3-1, are the navigation tree, alarm window, and map panel. This chapter describes general GUI operations such as opening and closing the GUI, managing windows and forms, and performing searches. See chapter 5 for information about map management.

Figure 3-1 Main 5620 SAM GUI elements



The 5620 SAM GUI enables an operator to do things such as the following:

- Display equipment and alarm status information.
- Configure and manage network management applications.
- Simplify the administration and configuration of equipment, customers, services, and subscribers using management forms instead of a CLI.
- Configure, manage, and monitor SLAs and equipment using statistics.
- Create and manage security policies for secure device and 5620 SAM access.

Floating windows

The 5620 SAM GUI uses floating windows that you can move, size, close, and bring to the foreground to provide the optimal working space for performing a task. By default, the navigation tree window appears at the left side of the GUI, the alarm window at the bottom, and the physical topology map is at the right side. If a window is closed or hidden, you can bring it to the foreground by selecting a toolbar icon or Window menu item, or by using shortcut keys. Each toolbar icon is identified by a tool tip that is displayed when the mouse pointer moves over the icon.

Main menu toolbar

The 5620 SAM GUI uses a main menu toolbar that you can use to create a shortcut to any main menu function. You can select which shortcut icons appear on the toolbar by right-clicking on the toolbar and selecting which icons to display.

User preferences

User preferences allow you to configure 5620 SAM GUI parameters to suit your specific requirements. Table 3-1 lists the location of user preference information in the 5620 SAM customer documentation suite. You can access the User Preferences form from the Application menu.

Table 3-1 Location of user preference information

Task	See
To set user preferences for configuration forms, show toolbar, default time zones, span of control, and topology windows	Section 3.5
To set user preferences for the alarm window	Procedures 37-5, 37-6, and 37-7
To access test objects that are available in the Service Test Manager (STM)	Procedure 78-3
To specify whether the 5620 SAM displays a confirmation message when an operator initiates a bulk change operation	Procedure 27-4
To specify the maximum number of objects to display per page on a list form	Procedure 3-35
To configure a browser path for a 5620 SAM client application to access the supervision portal from the 5620 SAM main menu	*5620 SAM Supervision Module User Guide*
To configure and view topology map icon labels to something other than the default value	Procedure 5-14

(1 of 2)

Task	See
To specify the global 5620 SAM parameters for graphing statistics	*5620 SAM Statistics Management Guide*
To set user preferences for script management	*5620 SAM Scripts and Templates Developer Guide*

(2 of 2)

System preferences

System preferences allow you to configure 5620 SAM system parameters to suit your specific requirements. Table 3-2 lists the location of system preference information in the 5620 SAM customer documentation suite. You can access the System Preferences form from the Administration menu.

Caution — Changing the parameter value of a System Preference may affect the behavior of an existing 5620 SAM service. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.

Note — The System Preferences parameters can only be modified by a user with administration privileges.

Table 3-2 Location of system preference information

Task	See
To configure the system preferences of the services that are associated with a customer	Procedure 67-2
To configure TCA system preferences	Procedure 26-5
To configure accounting and performance (Test Manager) statistics preferences	Section 38.4 and Procedure 78-2
To specify the storage parameters for exported statistics files on a 5620 SAM server	*5620 SAM XML OSS Interface Developer Guide*

Save workspace

You can save changes made to the navigation tree, the topology window, the alarm window, and the main menu toolbar with the save workspace function. Changes made to the position, size, and state preference of default windows can be saved. Shortcut icons added to the main menu toolbar can be saved. Each time you start the 5620 SAM GUI, the saved preferences are used instead of the defaults.

Note 1 — On a single-user client station, the GUI workspace preferences are saved in the following file:

- *user_home_dir*/5620SAM/guiPreference/*SAM_account_name*.guiPreferences on Solaris
- *user_home_dir*\5620SAM\guiPreference*SAM_account_name*.guiPreferences on Windows

where

user_home_dir is the home directory of the current user

SAM_account_name is the login name of the current 5620 SAM user

Note 2 — On a client delegate server station, the GUI workspace preferences are saved in the following file:

- *user_home_dir*/5620SAM/guiPreference/*SAM_account_name*.guiPreferences

where

user_home_dir is the home directory of the current user

SAM_account_name is the login name of the current 5620 SAM user

External windows

A window in the GUI can be used outside the GUI if you select the window and choose Move To External Window from the Window menu or from the menu that is displayed when you right-click on the window title bar.

External windows are managed by the operating system rather than the 5620 SAM. They maintain the window icon that is used within the GUI and are placed into a group of open 5620 SAM windows on the operating system task bar. Any windows launched from an external window appear as separate external windows. The 5620 SAM GUI task bar does not display external windows, but they can be viewed and brought to the front using the Window menu. The Window menu also contains options to Close All Internal Windows or Close All External SAM Windows.

Note — An external window cannot be moved back into the 5620 SAM GUI. You must close the external window and re-open it in the GUI.

Navigation tree

The navigation tree lists the managed equipment, services, and protocols that are configured on the NE. The navigation tree includes a view selector located on the navigation tree toolbar. The view selector is a drop-down menu that lists the physical and logical network views that are available.

The navigation tree is accessible from the main window, configuration forms, and maps.

See chapter 4 for more information about the navigation tree.

Contextual menus

Contextual menus allow you to create, configure, and manage specific parameters for the object and child objects from the navigation tree or from maps. You access the contextual menus by right-clicking on the navigation tree object or on the map object.

See chapter 4 for more information about contextual menus.

Task manager

The Task Manager allows SAM administrators and support personnel to monitor progress of operational tasks and SAM administrators to configure task monitoring parameters.

The Task Manager monitors the following:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

See Procedures 3-15 and 3-22.

Text message

Administrative users can send broadcast messages to some or all active GUI users logged into the 5620 SAM. This is useful for sending maintenance and similar notifications to active users.

See Procedures 3-23 and 9-31.

Maps

Each map displays network objects and information, and provides contextual menus to open forms that display additional information. In the context of a 5620 SAM map, a link object, such as a physical link or service tunnel, is called an edge. An object other than a link between objects, such as an NE or a topology group, is called a vertex.

See chapter 5 for more information on maps.

Alarm window

The alarm window allows you to view and manage incoming alarms from network components which are displayed in the dynamic alarm list and are associated with objects that represent the affected network components.

See chapter 37 for more information on the alarm window.

Forms

5620 SAM forms are used to do the following:

- configure device and 5620 SAM parameters
- display the status of an object
- perform FCAPS operations

A form can be displayed anywhere in the GUI. A newly opened form is displayed in the foreground. You can do the following:

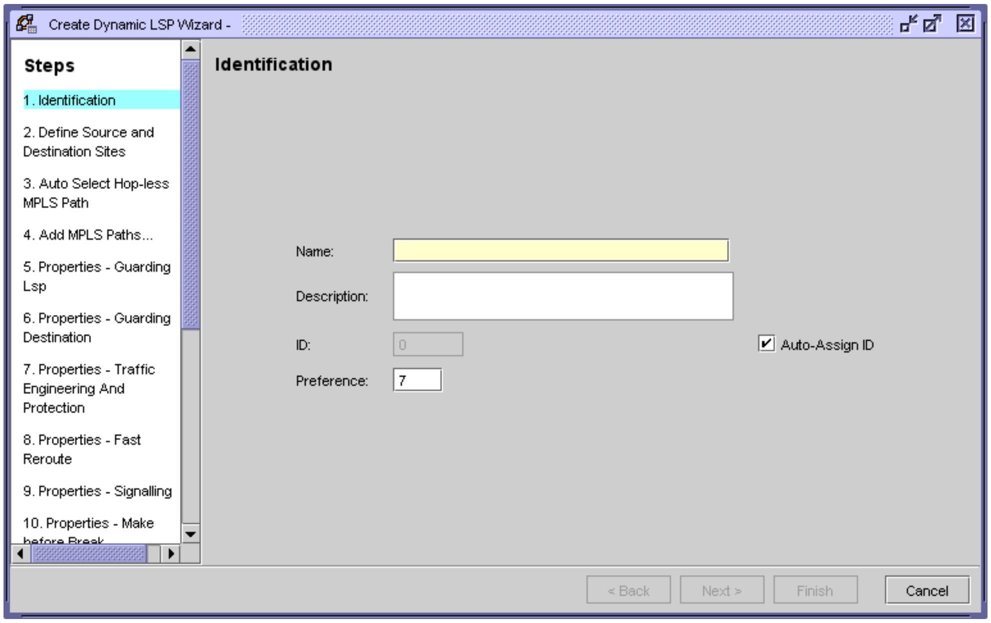
- organize forms according to operator preference
- compare information on multiple open forms
- navigate quickly to another open form by choosing the form from a list

A form has a title bar that displays object information. The displayed object name is the name specified during object creation. If the object is not named, a default name is used. When a form is minimized, a tool tip displays the title bar information. The Window menu lists the open forms.

Some configuration activities lead the operator through a series of forms, each of which represents a step in the configuration process. Such a form is called a step form. You must click on the Next button to proceed to the next step. Figure 3-2 shows the first step in a step form sequence. When the configuration sequence is complete, you must click on the Finish button to commit the changes. Each step must be performed to complete the configuration activity.

Note — Some steps open a new step form. You must complete the steps in the new form before you can return to the previous form. After you click on the Finish button, the previous form reappears.

Figure 3-2 Step form



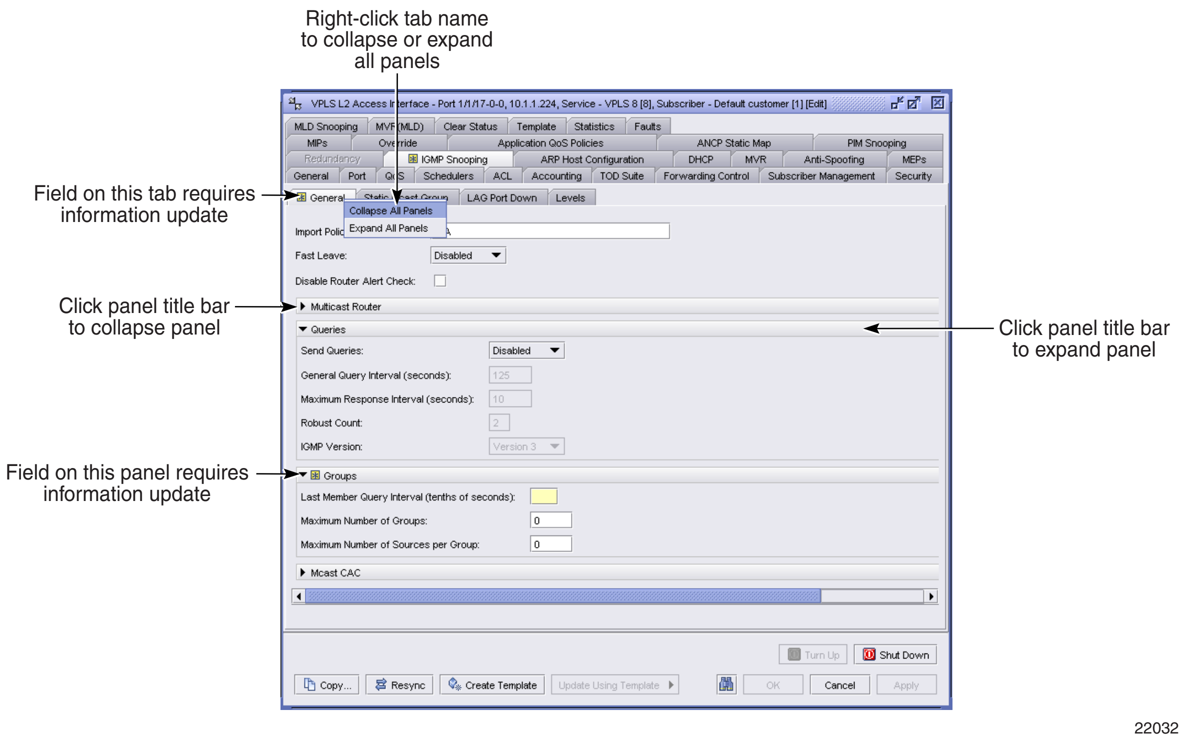
Collapsible panels

The 5620 SAM forms are used to configure devices. The 5620 SAM form panels can be collapsed to hide areas that are not of interest to the specific user or expanded to display all areas in a form.

To collapse a panel, click on the title bar of the expanded panel. To expand a collapsed panel click on the title bar of the collapsed panel, as shown in Figure 3-3. You can collapse or expand all of the panels on the form by right-clicking on the tab button title and then choosing the Collapse All Panels or Expand All Panels option.

An asterisk on a tab button or panel title bar indicates that a field contains incorrect data, or that a mandatory field requires data.

Figure 3-3 Collapsible panels in forms



Navigating service configuration forms

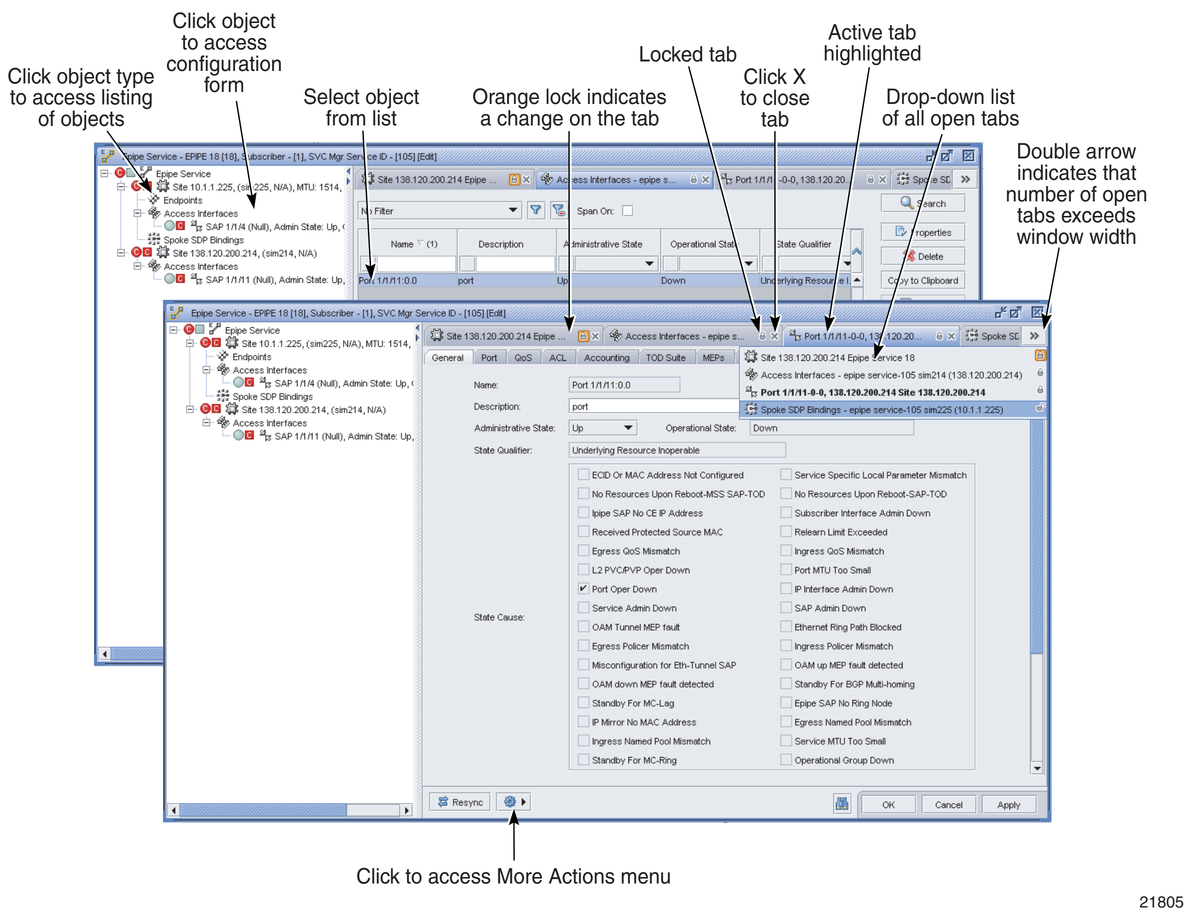
Service configuration forms allow you to create and manage services in the 5620 SAM. You can access service configuration forms from the Create menu or the Manage menu.

When you first access a service configuration form, the form displays a navigation tree on the left and the General tab on the right. The navigation tree lists the objects that are configured for the service. To access the configuration forms for the individual objects from the navigation tree, use one of the following methods:

- Click on the object type to access a filterable list form and choose the object.
- Click on the object in the navigation tree.

Figure 3-4 shows both methods of accessing object configuration forms from the navigation tree.

Figure 3-4 Service configuration form navigation



Navigating network element configuration forms

NE configuration forms allow you to create and manage network devices in the 5620 SAM. You can access NE configuration forms from the following locations:

- 5620 SAM GUI navigation tree
- Manage menu
- Physical topology map
- Service tunnel topology map

When you first access an NE configuration form, the form displays a navigation tree on the left and the General tab on the right. The navigation tree lists the devices that are configured on the NE. To access the configuration forms for the individual devices from the navigation tree, click on the object in the navigation tree.

See Chapter 4 for information about navigation tree capabilities.

Displaying multiple configuration forms

When you first access a configuration form, the form is unlocked. If you choose another object from the navigation tree, the unlocked form is replaced by the newly selected object configuration form. To lock the configuration form, click on the open lock icon on the configuration form tab, or right-click on the tab button and choose lock from the drop-down menu. When the configuration form is locked, the form remains open until the user closes the form. You can add configuration forms to the window by choosing objects from the navigation tree and then locking each form.

Note — Locked forms can only be closed (and not unlocked).

Each form is represented by a tab. If the tabs of the open forms exceed the width of the window, double arrows are displayed. Click on the double arrows to display a drop-down menu of the open configuration forms. You can access the open configuration forms from the drop-down menu or from the tab buttons. Figure 3-4 shows multiple open service configuration forms and the navigation options.

Object configuration forms can be undocked from the main configuration form window by right-clicking on the component tab title and selecting Undock. The undocked form opens in a new window and the configuration form tab is removed from the main configuration form window. Any changes that are made on the undocked object configuration form are immediately sent to the server.

Note 1 — The root object of the configuration form cannot be undocked, for example the IES service configuration form.

Note 2 — List forms cannot be undocked, for example a listing of access interfaces on a site.

Note 3 — Undocking is not supported on (Create) forms.

When the mouse point moves over the object form label, a tool tip displays a descriptive label for the form.

Modified configuration forms

If a configuration form is modified, the form changes to locked and the lock icon appears in orange to indicate that a modification occurred.

For service configuration forms, if an object is added to the service configuration, the new object appears in the navigation tree and the configuration form is displayed with the orange lock icon. The icon remains orange until the modifications are saved or discarded.

For equipment configuration forms, if an object is added from the navigation tree, the change will be made immediately. However, if a change, such as adding or removing an object, is made to an equipment configuration form, the change will be reflected on the form immediately, but it will not be reflected on the navigation tree until the Apply Tab, OK, or Apply button has been pressed.

Note — For the NE and composite service configuration forms, changes implemented by pressing the Apply Tab button apply only to the current object-level tab. Changes implemented by pressing the OK, Apply, or Cancel buttons apply to the entire form.

If you attempt to close a modified configuration form that contains unsaved changes, a message prompts you to specify whether to discard the changes or return to the display. If you attempt to close a modified configuration form that has related forms with unsaved modifications, the message lists the forms that have unsaved changes.

Localized language support

The 5620 SAM GUI supports localized language display. Localized language display, also known as internationalization, displays 5620 SAM GUI text in a specified language. The localized language setting applies to most 5620 SAM GUI objects except system components and database objects. Contact Alcatel-Lucent support for more information about localized language support.

Note 1 — The 5620 SAM supports localized language settings using predefined strings, and does not translate data to different languages.

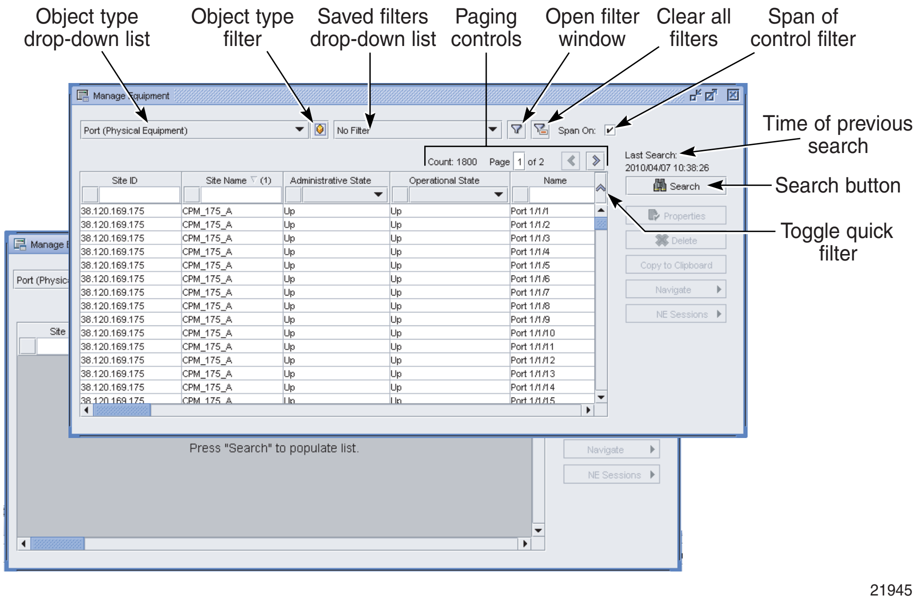
Note 2 — The 5620 SAM-O does not support language localization.

3.2 Using search functions

You can search for many types of objects using list forms, maps, and the navigation tree. For lists that do not populate automatically, the message "Press "Search" to populate list." displays in the result panel when you first access the list form. After you perform a search, a list form or map enables you to manage the results, for example, view or edit object information, or delete objects. Figure 3-5 shows a filterable list form that displays the following above the listed items:

- number of returned search items
- time of the most recent search
- filter controls for refining the list of returned search items
- paging controls for browsing through multiple pages of returned search items

Figure 3-5 Filterable list form



When the number of search results exceeds the allowed limit, the 5620 SAM displays a dialog box that indicates the number of results returned. You can use filter options to refine the search criteria and limit the search results.

A search returns one page of results at a time. You can configure the number of items per page on the User Preferences form. The paging controls on a list form become active when the number of items returned exceeds the page limit. You can use these controls to move sequentially through the pages of listed information or jump directly to a specific page.

You can save and reuse multiple search filters in list forms and maps. Only the saved filters of the current object type and ancestor types are available. You can use an advanced filter form to refine the search criteria using literal values, and different kinds of operators, such as arithmetic and Boolean.

Note — A tab that lists timestamped information, such as the Statistics tab of a 5620 SAM properties form, contains a default saved filter for statistics collected in the most recent time period, for example, the last hour. The time period depends on the type of object specified in the object type drop-down list. See chapter 6 for more information on how to change the time period, from its default value.

See chapter 5 for information about creating map filters.

Using search filters

When you perform a search from a list form, you can configure filters. A filter is based on a combination of attributes, functions, and values. When searching for objects with an ID value, you can search based on LESS THAN, EQUAL TO, or GREATER THAN. For text-type parameters, you can use advanced search functions, such as EQUALS or CONTAINS. Consider the following.

- You can set filters based on letters, numbers, and special characters.
- The search filters are typically case-insensitive; a search on 'ABC' and 'abc' returns the same list. WILDCARD searches, however, are case-sensitive.

Table 3-3 describes the operation of available 5620 SAM search functions.

Table 3-3 Search functions

Operator	Description
APPROXIMATELY EQUAL	When set to APPROXIMATELY EQUAL, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that match the specified time criterion, which you can specify using 1m resolution.
CONTAINS	When set to CONTAINS, the search returns only items that match the entered value. For example, a Description CONTAINS search of 'AB' returns 'ABC Industries' and 'Calgary, AB'. Any empty CONTAINS search returns all items. This search parameter is not case sensitive.
DOES NOT CONTAIN	When set to DOES NOT CONTAIN, the search returns only items that do not match the entered value. For example, a Service Name DOES NOT CONTAIN search of 'epipe' returns only services such as 'IES' services that do not contain 'epipe' as part of the service name. This search parameter is not case sensitive.
EQUALS	When set to EQUALS, the search returns only items that equal the value; for example, Administrative State set to 'Down".
GREATER OR EQUAL	When set to GREATER OR EQUAL, the search returns only items that have a value greater than or equal to the specified criteria.
GREATER THAN	When set to GREATER THAN, the search returns only items that have a value greater than the specified criteria.
IN THE PAST	When set to IN THE PAST, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that have a timestamp that is between the specified time and the present. Click on the clock icon beside the column heading filter field to specify a time criterion.
LESS OR EQUAL	When set to LESS OR EQUAL, the search returns only items that have a value less than or equal to the specified criteria.
LESS THAN	When set to LESS THAN, the search returns only items that have a value less than the specified criteria.
MATCHES ALL	When set to MATCHES ALL, the search returns only items that equal the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match all of the selected property values.
MATCHES ANY	When set to MATCHES ANY, the search returns only items that equal at least one of the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match one or more of each of the selected property values.

(1 of 2)

Operator	Description
NOT EQUAL	When set to NOT EQUAL, the search returns only items that do not match the selected criteria.
WILDCARD	When set to WILDCARD, you can use the ? character as a single-character wildcard, and * as a multi-character wildcard. For example, a Description WILDCARD search of 'VPRN ?' returns 'VPRN 4' and 'VPRN 8', but not 'VPRN Texas'.

(2 of 2)

Searches using Boolean operators

You can perform advanced searches that use multiple criteria to obtain more precise results. Boolean operators are used to limit and expand searches to the criteria that are specified in the search expressions. Boolean operators can be nested to combine several search expressions into one search expression.

Table 3-4 lists and describes the Boolean search operators.

Table 3-4 Boolean search operators

Boolean operator	Description
AND	When set to AND, the search returns only items that meet all of the specified search criteria.
OR	When set to OR, the search returns only items that meet at least one of the specified search criteria.
NOT	When set to NOT, the search returns only items that do not meet the specified search criteria.

Invalid attributes or values

When a saved search filter contains attributes or values that are not available for the object being searched, the invalid attributes or values are displayed in red text in the filter window. As long as invalid attributes or values exist, the Save button of the filter window are disabled. When a filter with invalid attributes or values is applied, the invalid attributes are not evaluated. For information about using the filter window, see Procedure 3-27.

When a saved search filter contains an invalid attribute, the attribute, function, and value are all displayed in red text in the filter window. The attribute are is surrounded by "**". Both the attribute and value are displayed as a best effort string and may not be internationalized.

When an invalid attribute is selected, the Attribute drop-down is displayed a best effort string that may not be internationalized. If the attribute is not recognized, the Functions drop-down and the Value field display only the corresponding values that are displayed in the filter window. These values cannot be changed until a different attribute is chosen from the Attribute drop-down, at which point they are updated accordingly.

When a saved search filter contains only an invalid value, only the value itself is displayed in red text. The value is surrounded by “**” and may not be internationalized. The Value drop-down does not display a value, but is populated with valid values that can be used to update the filter.

When a saved search filter contains invalid attributes, the filter name is displayed in red text in the saved filters drop-down of a list form. When a filter with invalid attributes is applied from the saved filters drop-down, the invalid attributes are not evaluated. For information about using the saved filters drop-down list, see Procedure 3-39.

Preset filters

When a preset filter is ready to be applied, the saved filters drop-down menu displays an italicized No Filter. Opening the filter window displays the preset filter. Clicking on the Search button applies the filter, and clicking on the Clear All Filters button clears the filter.

Span of control filters

A 5620 SAM GUI user can filter the objects that a map or list form displays, based on the user span of control. By default, the GUI displays only the objects that are in the View Access and Edit Access spans of the user.

Most 5620 SAM list forms contain a configurable Span On parameter. When the parameter is enabled, the displayed objects are limited to the Edit Access span objects. The parameter setting overrides, on the current form only, the global span of control filter setting on the User Preferences form. When the Span On parameter is displayed on a list form that allows filter creation, the associated filter form contains a drop-down menu that has the following options:

- Span: On—Only Edit Access span objects are displayed.
- Span: Off—View Access and Edit Access span objects are displayed.
- Span: User Preference—The User Preferences span filter setting determines which objects are displayed.

The Span On parameter setting in a list form defaults to the User Preferences span filter setting. 5620 SAM topology maps, however, do not contain the Span On parameter; instead, they automatically filter the NEs according to the User Preferences span filter setting.

See chapter 9 for information about spans of control. See Procedure 3-13 for information about configuring the global span of control filter on the User Preferences form.

Equipment group filters

The equipment group filters allow you to search globally for new alarms, historical alarms, managed equipment objects, and managed service objects by equipment that is organized by topology group. See Procedure 5-29 for information about how to create a topology group.

The equipment group filter is created by choosing existing topology groups. The filters can be saved, modified, or deleted. See Procedures 3-41 and 3-42 for information about how to use the equipment group filters .

Equipment group filters can return up to 12 000 elements. If the limit is exceeded, the user is prompted to modify the filter to reduce the number of elements within the limit. Additionally, if you choose an equipment group filter that includes a topology group that has been modified since the filter was applied, an icon appears beside the equipment group filter drop-down list prompting you to press the Search button to update the filter.

Locating attributes on configuration forms

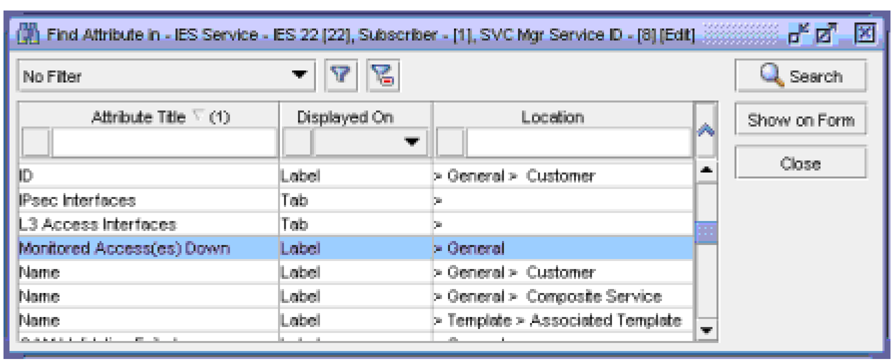
The find attribute function allows you to locate specific attributes on a configuration form.

Note — In this context, attribute refers to the names of tabs, panels, or fields.

Using the Find button located in the bottom right of a configuration form, you can list the attributes in that form. The Find Attribute in list form includes the name, type, and location for all attributes on the configuration form. After you choose the attribute using one of the selection methods described in Procedure 3-30, the tab where the attribute resides appears and the attribute name is highlighted. After you close the list form, the attribute name returns to the default display color. Figure 3-6 shows the Find Attribute in list form.

Note — For configuration forms that can display multiple objects simultaneously, such as the service configuration forms, the search is performed only on the selected object.

Figure 3-6 Find Attribute in list form



3.3 Workflow to use 5620 SAM GUI

1. Start the 5620 SAM GUI. See section 3.4 for more information.
2. Configure the way that the GUI operates for one or more users. See section 3.5 for more information.

3 Manage objects using 5620 SAM main menu options, the alarm and map windows, and the navigation tree. See section 3.6 for more information.

4 Use list forms to perform filtered searches that return information, and optionally save the filters and listed information to files. See section 3.7 for more information.

3.4 5620 SAM GUI start up procedures

The following procedures describe how to start up the 5620 SAM GUI.

Procedure 3-1 To start the 5620 SAM client GUI on a Windows single-user client station

Perform this procedure to start the 5620 SAM single-user client software on a Windows station and begin using the client GUI.

Note 1 — You can have more than one client installed on a station, but you can run only one client instance at a time. For example, you can have a Release 8.0 R1 client and a Release 9.0 R1 client running on the same station, but you cannot have two Release 9.0 R1 clients running on the same station.

Note 2 — The user that starts a 5620 SAM Windows client must be one of the following:

- the user that installed the client software
- a user with sufficient permissions on the client files and directories, such as a local administrator

1 To start the client GUI using a web browser, perform the following steps.

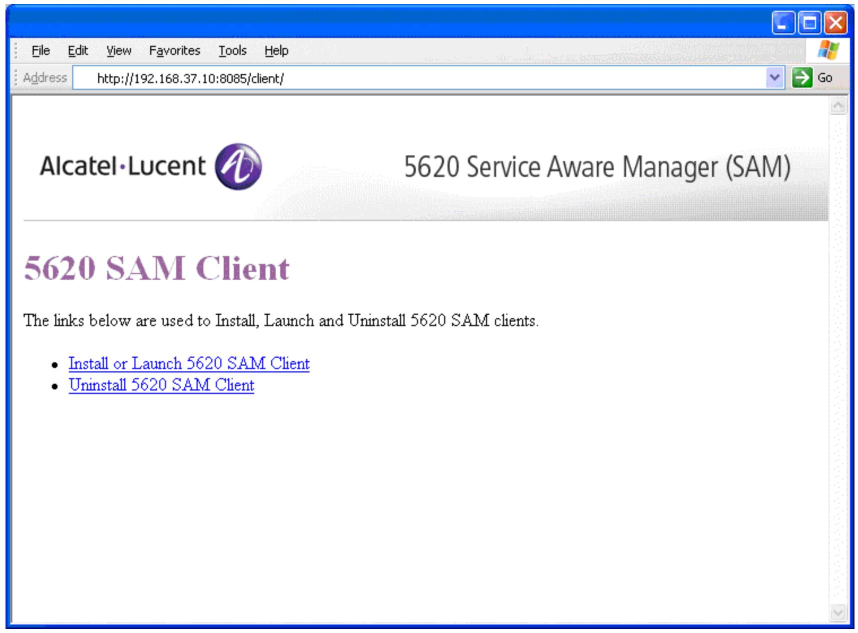
i Navigate to the following URL on the 5620 SAM main server:

http://*server*:8085/client

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 3-7 is displayed.

Figure 3-7 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation directory. Use the form to specify the client installation directory, for example, C:\5620sam\client.

iv The 5620 SAM login form opens. Go to step 5.

2 To start the client GUI using a desktop shortcut, perform the following steps.

i Double-click on the 5620 SAM Client App icon on the Windows desktop. The 5620 SAM client login form opens.

ii Go to step 4.

3 To start the client GUI using a CLI, perform the following steps.

Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a command window.

ii Navigate to the 5620 SAM client installation directory. Enter the following commands at the CLI prompt in the order shown:

drive_ID ↵

cd *install_dir*\nms\bin ↵

where
drive_ID is the drive on which the 5620 SAM client is installed, for example, C:
install_dir is the 5620 SAM client installation location, typically \5620sam\client

iii Enter the following at the CLI prompt to start the 5620 SAM client using one or more startup options:

nmsclient.bat *option* ↵

where *option* is one or more of the startup options listed in Table 3-5

For example, to force a client update, enter the following:

nmsclient.bat update ↵

Table 3-5 5620 SAM client startup options for Windows

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.
retryCount	Starts the client and specifies the number of times to attempt to download a client update
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.

(1 of 2)

Option	Description
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*\nms\config directory where *install_dir* is the 5620 SAM client installation directory, typically C:\5620sam\client After this option is specified, it remains in effect until the client is started using the "update" option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*\nms\config\keepFile.txt are not to be overwritten during a client update where *install_dir* is the 5620 SAM client installation location, typically C:\5620sam\client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s. The maximum connection timeout in Windows is 20s.
readTimeout [*timeout*]	Specifies a timeout value, in seconds, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s. The maximum read timeout in Windows is 20s.
help	Displays the nmsclient.bat usage information and options

(2 of 2)

The 5620 SAM client login form opens.

4 Choose the 5620 SAM server that you want to log in to from the Server drop-down list.

Note — Before the login form can display multiple servers in the Server drop-down list, you must configure the client to support multiple server options. See chapter 6 for more information.

5 Enter the Login name and Password information required for the server.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login name and password used depend on whether client GUI users are authenticated locally or remotely, as determined by the system administrator. Use the login name and password provided by your system administrator. See chapter 9 for more information.

6 Click on the Login button. The 5620 SAM GUI opens.

7 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you want to remove an older version of JRE. If this occurs, perform one of the following.

a If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.

b If the client is required for connecting to a a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the *5620 SAM Troubleshooting Guide*.

Procedure 3-2 To start the 5620 SAM client GUI on a Solaris single-user client station

Perform this procedure to start the 5620 SAM single-user client software on a Solaris station and begin using the client GUI.

Note 1 — You can have more than one client installed on a station, but you can run only one client instance at a time. For example, you can have a Release 8.0 R1 client and a Release 9.0 R1 client running on the same station, but you cannot have two Release 9.0 R1 clients running on the same station.

Note 2 — The user that starts a 5620 SAM Solaris client must be one of the following:

- the user that installed the client software
- another user that has read, write, and execute permissions on the client files and directories

1 To start the client GUI using a web browser, perform the following steps.

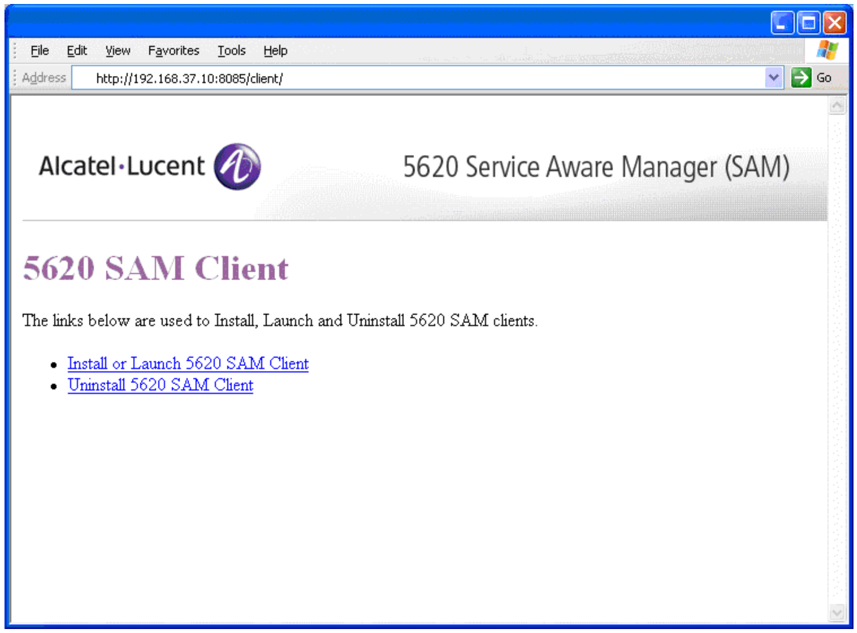
i Navigate to the following URL on the 5620 SAM main server:

http://*server*:8085/client

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 3-8 is displayed.

Figure 3-8 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation location. Use the form to specify the current client installation directory, for example, /opt/5620sam/client.

iv The 5620 SAM login form opens. Go to step 5.

2 To start the client GUI using a desktop shortcut, perform the following steps.

i Double-click on the 5620 SAM Client App icon on the desktop. The 5620 SAM client login form opens.

ii Go to step 4.

3 To start the client GUI using a CLI, perform the following steps.

Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a bash console window on the client station.

ii Enter the following at the CLI prompt to navigate to the 5620 SAM client installation directory:

cd *install_dir*/nms/bin ↵

where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client

iii To specify one or more client startup options, enter the following at the CLI prompt:

./nmsclient.bash *option* ↵

where *option* is one or more of the startup options listed in Table 3-6

For example, to force a client update, enter the following:

./nmsclient.bash update ↵

Table 3-6 5620 SAM client startup options for Solaris

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.
retryCount	Starts the client and specifies the number of times to attempt to download a client update
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.

(1 of 2)

Option	Description
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*/nms/config directory where *install_dir* is the 5620 SAM client installation directory, typically /opt/5620sam/client After this option is specified, it remains in effect until the client is started using the “update” option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*/nms/config/keepFile.txt are not to be overwritten during a client update where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s.
readTimeout [*timeout*]	Specifies a timeout value, in seconds, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s.
help	Displays the nmsclient.bash usage information and options

(2 of 2)

The 5620 SAM client login form opens.

4 Choose the 5620 SAM server that you want to log in to from the Server drop-down list.

Note — Before the login form can display multiple servers in the Server drop-down list, you must configure the client to support multiple server options. See chapter 6 for more information.

5 Enter the Login name and Password information required for the server.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login credentials that are required depend on whether local or remote user authentication is used for the GUI client. Use the login name and password provided by your system administrator. See chapter 9 for more information.

6 Click on the Login button. The 5620 SAM GUI opens.

7 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you want to remove an older version of JRE. If this occurs, perform one of the following.

- **a** If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.
- **b** If the client is required for connecting to a a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the *5620 SAM Troubleshooting Guide*.

Procedure 3-3 To start the 5620 SAM client GUI through a client delegate server

Perform this procedure to open a 5620 SAM client GUI using the 5620 SAM client delegate software on another station.

1 If you are not in the same physical facility as the client delegate server, log in to the facility using the appropriate third-party access tool, for example, Citrix software.

2 Log in to the client delegate server using an account with local user privileges.

3 Open a bash console window on the client delegate server station.

4 Use the appropriate UNIX commands to redirect the display to the station that you are using.

5 Enter the following at the CLI prompt to navigate to the 5620 SAM client installation directory on the client delegate server:

cd *install_dir*/nms/bin ↵

where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client

6 Perform step 3 of Procedure 3-2.

Note — You must be logged in as the samadmin user on a client delegate server to use a client startup option that updates the client software or configuration. If you attempt such an operation as a user other than samadmin, the operation fails.

7 Enter the Login name and Password information on the 5620 SAM client login form.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login credentials that are required depend on whether local or remote user authentication is used for the GUI client. Use the login name and password provided by your system administrator. See chapter 9 for more information.

8 Click on the Login button. The 5620 SAM client GUI opens.

If you have trouble opening the GUI, see the Troubleshooting 5620 SAM Clients chapter of the *5620 SAM Troubleshooting Guide*.

Procedure 3-4 To change to a different 5620 SAM client GUI user

Perform this procedure to change which 5620 SAM user is currently logged in to the client GUI.

1 Choose Application→Switch User from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI restarts and displays the login form.

3 Log in using the required credentials. The client GUI opens.

Procedure 3-5 To close the 5620 SAM GUI

1 Choose Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI application closes.

3.5 5620 SAM GUI configuration procedures

The following procedures describe how to configure 5620 SAM GUI operation.

Procedure 3-6 To configure the default client time zone

Perform this procedure to specify which time zone the 5620 SAM client will use by default.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Default Client Time Zone parameter.

3 Click on the OK button. The User Preferences form closes and a dialog box appears.

4 Click on the OK button.

Procedure 3-7 To configure the current client time zone

Perform this procedure to specify which time zone the 5620 SAM client will use currently.

1 Click on the Current Client Time Zone button in the bottom right hand corner of the GUI. The Current Client Time Zone form opens.

2 Perform one of the following:

a Select Use Default Client Time Zone.

b Select Use Specific Client Time Zone and choose a time zone from the list.

3 Click on the OK button. The Current Client Time Zone form closes and a dialog box appears.

4 Click on the OK button.

Procedure 3-8 To configure the GUI inactivity timeout

A 5620 SAM user with an admin scope of command role can configure a GUI inactivity check that applies to all client GUIs, or to sets of users based on the associated user groups.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 To change the GUI inactivity check for all 5620 SAM GUI users, perform the following steps.

i Configure the Client Timeout (minutes) parameter.

ii Click on the Apply button.

3 To change the GUI inactivity check for all users in a user group, perform the following steps.

i Click on the User Groups tab. A list of user groups is displayed.

ii Choose a user group from the list and click on the Properties button. The User Group *name* (Edit) form opens.

iii Enable the Override Global Timeout parameter.

iv Configure the Client Timeout (minutes) parameter.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The User Group (Edit) form closes.

4 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 3-9 To show, hide, or modify the toolbar

Icons that represent a subset of the main menu functions are available in the toolbar.

1 Start the 5620 SAM GUI. By default, toolbar icons are displayed under the 5620 SAM main menu.

2 To show the toolbar when it is hidden, perform the following steps.

i Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

ii Select the Show Toolbar parameter and click on the OK button.

3 To modify the toolbar, right-click on an empty section of the toolbar. The toolbar contextual menu is displayed.

4 Perform one of the following:

a To add icons to the toolbar, select the icons in the contextual menu. The icons are added to the toolbar.

b To remove icons from the toolbar, deselect the icons in the contextual menu. The icons are removed from the toolbar.

c To hide the toolbar, choose Hide Toolbar from the contextual menu. The toolbar is removed from the display.

5 Click on an empty section of the GUI to close the toolbar contextual menu.

Procedure 3-10 To enable or disable containing window warnings

1. Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
2. Configure the Suppress Containing Window Warning parameter.
3. Click on the OK button. The User Preferences form closes.

Procedure 3-11 To enable or disable template generation messages

1. Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
2. Configure the Suppress Template Generation Message parameter.
3. Click on the OK button. The User Preferences form closes.

Procedure 3-12 To enable or disable Service and Composite Service Topology Map Load Warnings

1. Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.
2. Configure the Suppress Service and Composite Service Map Load Warning parameter.
3. Click on the OK button. The User Preferences form closes.

Procedure 3-13 To enable or disable a global span of control filter

Perform this procedure to configure which objects the 5620 SAM client GUI displays in frames that include list forms, maps, and the Alarm Window. By default, the GUI displays all objects that are in your View Access and Edit Access spans.

You can temporarily override the global filter setting in a list form or window using the Span On check box, and can include your span of control in an advanced filter window. See section 3.2 for information about performing searches using list forms and span of control filters.

Note — This procedure affects the GUI display of only the user that performs the procedure, and not other users.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Configure the Apply User Span of Control parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 3-14 To save the GUI workspace preferences

Perform this procedure to save the current GUI workspace preferences. The next time you log in to the client on the same user account and workstation, your GUI workspace preferences are restored.

1 Configure the following GUI workspace elements, as required:

- position, size, and state of the navigation tree, alarm window, and physical topology
- toolbar settings

2 Choose Application→Save Workspace from the 5620 SAM main menu. The current GUI workspace preferences are saved.

Procedure 3-15 To configure the 5620 SAM Task Manager

The Task Manager allows 5620 SAM operators to monitor progress of operational tasks. Only the 5620 SAM administrators can configure task monitoring parameters. The Task Manager monitors the following:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

Note — The Task Manager is operational with the default values.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Open the nms-server.xml file using a text editor.

4 Find and configure the parameters to fit your operational requirements.

- maxNumRetainedTasks
- numTasksToPurgeWhenFull
- successfulTasksPurgeInterval
- failedTasksPurgeInterval

Note — If one or more of the parameters are changed from their default values, you must restart the 5620 SAM server for the changes to take effect.

5 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config.

6 Open the nms-client.xml file using a text editor.

7 If required, configure the autoRefreshInterval parameter. The parameter does not take effect until the 5620 SAM client is restarted.

8 If required, export a report to a file, as described in Procedure 3-34.

9 If required, save the table preferences, as described in section 3.2.

10 Close the form. See Procedure 3-22 to view the Task Manager.

3.6 Basic 5620 SAM GUI operation procedures

The following procedures describe how to operate and navigate the 5620 SAM GUI.

Procedure 3-16 To open the navigation tree or alarm window

The navigation tree and alarm window position and state preferences are stored in the local file system so that each time the GUI is opened using the same user account, the saved preferences are used.

1 Start the 5620 SAM client GUI.

2 Open a hidden window or bring these windows to the foreground using one of the following methods:

- **a** Choose the Navigation Tree or Alarm Window icon from the toolbar.
- **b** Choose *View*-Network or Alarm Window from the Window menu.
- **c** Use the Navigation Tree or Alarm Window shortcut key.
- **d** Choose the icon that represents the window from the task bar. The task bar is located just above the status bar.

Procedure 3-17 To go to a window

1 Perform one of the following:

- **a** Copy a window identifier link to the clipboard. See Procedure 3-24 for more information.
- **b** Save a window identifier link to the clipboard. See Procedure 3-25 for more information.

2 Choose Application→Go To Window from the 5620 SAM main menu. The Go To Window window opens.

3 Click on the Paste button or press CTRL+V. The window link identifier appears in the Label area.

4 Perform one of the following:

- **a** Click on the OK button. The Go To Window window closes and the window specified in step 1 opens.
- **b** Click on the Apply button. The window specified in step 1 opens.

Procedure 3-18 To use menus, the toolbar, or shortcuts

1 Start the 5620 SAM GUI.

2 Perform one of the following to open an object.

a Choose an option from the main menu. A shortcut icon for the menu option is shown beside the option text.

b Click on the menu equivalent in the toolbar. Scroll over the toolbar icons to view a tool tip that describes the icon function. See Procedure 3-9 for information about modifying or hiding the toolbar.

c By typing the appropriate ALT+*Key* shortcut; the underlined letter in a main menu item is the shortcut key. For example, ALT+P opens the Policies menu.

Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

Procedure 3-19 To use menus, windows, and forms to configure or view parameters

1 Start the 5620 SAM client GUI.

2 Open a configuration form using one of the following methods.

a Double-click on the lowest-level navigation tree object to open the object properties form. When you double-click on an object that has child objects, the child object is revealed; when you double-click on an object that has no child objects, the object properties form opens.

b Choose the appropriate 5620 SAM main menu or submenu option.

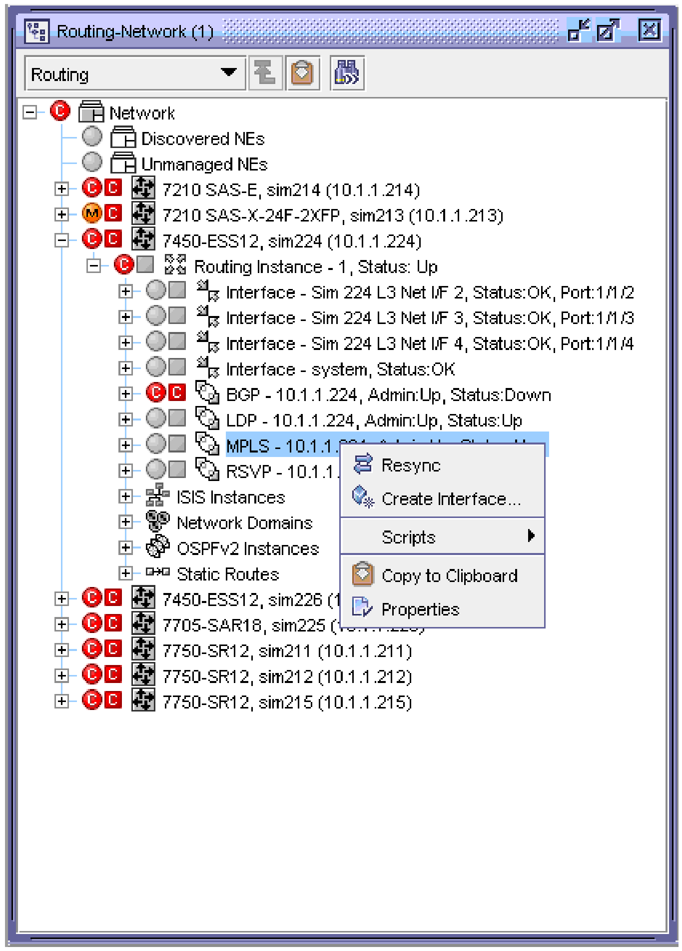
c Double-click on an object, for example, a customer in a list of customers.

d Click on the task bar icon that represents the form.

e Right-click on an object in the navigation tree or Alarm Window and choose the appropriate option from the contextual menu.

Figure 3-9 shows an example of a right-click contextual menu in the navigation tree.

Figure 3-9 Right-click contextual menu example



The appropriate form opens.

3 Configure or view the parameters on the form, as required, using the following methods.

Note — A parameter that has a yellow background is mandatory and must be configured before you can go to the next form or apply the changes on the current form.

a Enter information beside the parameter, as appropriate. For example, type in text to configure the Description parameter.

b Use the drop-down menu to choose an option from a list. For example, choose Access as the port mode on a port configuration form.

c If the configuration form is a step form, follow the form prompts.

d Double-click an object in a row to open a new view or set of configurations. For example, from a list of ports double-click on a row to open the configuration form for that port.

e Right-click on an object in the navigation tree to display additional contextual menu choices, as shown in Figure 3-9.

See the *5620 SAM Parameter Guide* for a list of the configurable parameters.

4 Click on the Apply button to save the configuration changes without closing the form.

5 Click on the appropriate button to complete the configuration.

a Click on the OK button to save the changes and close the form, if the form is other than a step form.

b Click on the Finish button to save the changes in a step form.

c Click on the More Actions button and choose Turn Up to activate the object.

d Click on the More Actions button and choose Shut Down to deactivate the object.

e Click on the Cancel button to close the form without saving the changes.

f Click on the Close button to close the form without saving the changes.

Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

g The Resync button to ensure that the 5620 SAM and managed devices are synchronized. Resynchronization does not affect the contents of the historical statistics database.

Procedure 3-20 To arrange multiple open forms

1 To arrange multiple open forms so that they overlap, choose Window→Cascade from the 5620 SAM main menu. The forms are displayed in the top left area of the GUI with the form that is farthest to the right in the foreground.

2 To arrange multiple open forms so that they do not overlap, perform one of the following.

a Choose Window→Tile Vertical from the 5620 SAM main menu. The forms are displayed beside each other.

b Choose Window→Tile Horizontal from the 5620 SAM main menu. The forms are displayed above each other.

c Choose Window→Tile Square from the 5620 SAM main menu. The forms are displayed beside and above each other to fill the GUI workspace.

3 To move an open form to the foreground, perform one of the following.

a Click on the task bar icon that represents the open form.

b Choose Window→*form_name* from the 5620 SAM main menu

where *form_name* is the name of the form that you want in the foreground

Procedure 3-21 To close one or all open forms

Note — When there is unsaved information on a form, you are prompted to save the changes before you close the form.

1 To close one form, perform one of the following.

a Click on the X in the top-right corner of the form.

b Click on the Close button.

c Right-click on a form in the task bar and choose Close from the contextual menu.

2 To close all open forms, choose Window→Close All from the 5620 SAM main menu.

Procedure 3-22 To view the 5620 SAM Task Manager

See Procedure 3-15 to configure the Task Manager.

Note — You can send the tasks that the Task Manager displays to a file using the OSSI findToFile method. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

1 Choose Application→Task Manager from the 5620 SAM main menu. The Task Manager form opens.

The All Users check box appears for only the 5620 SAM administrators. If you are a 5620 SAM administrator or a user with an assigned administrator scope of command role, go to step 2 to monitor tasks for all users. Otherwise, go to step 3.

2 Enable the All Users check box to monitor operations that are performed in the 5620 SAM server by all 5620 SAM users. The default is Disabled.

3 If required, configure the filter and click on the Search button. The following appear in the Task Manager:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

Note — The Task Manager automatically refreshes when the value of the autoRefreshInterval parameter is reached. The default is 20 s. You can also click on the Search button to refresh the list of tasks.

4 Double-click on a task to view more information about the task. The Task - Top Level window opens.

5 Click on the Tree tab button to view a hierarchical display of the tasks.

6 Click on the Sub-Tasks tab button to view the sub-tasks that are associated with the task.

7 Click on the More Actions button and choose Activity Log to open the User Read Log or User Request Log form and view additional information relating to the task.

The Activity Log option is available only for Top Level task forms. It is not available for sub-task forms.

8 Close the form.

Procedure 3-23 To send a text message to another 5620 SAM user

You can send text messages to another 5620 SAM user or to all active users logged into the 5620 SAM.

1 Choose Application→Text Message from the 5620 SAM main menu. The Text Message window opens.

2 Type the text message in the text area.

Note — You can also press CTRL+V to paste information from the clipboard into the text area. For example, pasting a window link identifier creates a link which the recipient can click to launch the window. For more information about copying to the clipboard, see Procedures 3-24 and 3-25.

3 Click on the Send To... button. The Select Session window opens.

4 If required, configure the filter criteria to create a filtered list of GUI client sessions.

5 Click on the Search button. A list of active GUI client sessions is displayed.

6 Perform one of the following:

- **a** To select a single user, click on a GUI client session.
- **b** To select all GUI client sessions, press CTRL +A
- **c** To select non-consecutive GUI client sessions, click on a session and press CTRL +ALT and select another session.

7 Click on the OK button. The text message is sent to the selected client(s). Messages are uniquely identified with the Client ID number of the sender. You can reply back to the sender by clicking on the Reply button.

Procedure 3-24 To use the clipboard

1 Select one or more objects to copy from one of the following locations.

- **a** To copy objects from the equipment view of the navigation tree, go to step 2.
- **b** To copy objects from a generated or displayed list, go to step 2.
- **c** To copy objects from a read-only field on a configuration form, go to step 6.

2 Click on the Copy to Clipboard button. The object properties are copied to the clipboard.

3 Choose Application→Clipboard from the 5620 SAM main menu. The Clipboard window opens displaying the copied object properties in a text string format.

4 Perform one of the following:

a Copy and paste the properties text string to an external application.

i Select the properties text string that you want to copy and press CTRL+C.

Only one text string can be selected and copied at a time.

ii Paste the properties text string into an external application.

b View the property form for a copied object.

i Select the properties text string for the object that you want to view.

ii Click on the View Object button. The properties form for the object opens.

5 Repeat steps 1 to 4 to copy additional objects, or close the Clipboard window.

For information about using the clipboard function to create physical links, see Procedure 5-34.

6 Highlight a read-only field to copy and press CTRL+C.

7 Paste the copied read-only field into another form or application by pressing CTRL+V.

Note — You cannot copy a password field.

Procedure 3-25 To save a window to the clipboard

1 Open a configuration form.

2 Choose Application→Save Window To Clipboard from the 5620 SAM main menu. The window identifier link is saved to the clipboard.

3.7 5620 SAM GUI search procedures

The following procedures describe how to use the 5620 SAM to search for and display information.

Procedure 3-26 To perform a simple search using column headings

1 Open a list form.

2 If available, choose an entry from the object drop-down list.

> **Note —** If you click on the Search button without selecting a specific object type from the list, a default entry may be used.

3 If the filter has not been pre-populated, configure the filter criteria using the filter area of any column heading.

> **Note 1 —** Entering a value into a filter area of a column heading without specifying an operation from an operation drop-down menu causes a default operation to be automatically selected.
>
> **Note 2 —** The following operators are available for filtering a list by object timestamp. Each operator allows you to specify the time criteria using the clock icon beside the column heading filter:
>
> - APPROXIMATELY EQUAL, which allows you to specify a time with 1m resolution rather than the default 1ms timestamp resolution
> - IN THE PAST, which allows you to specify an amount of time before the present as the filter range, for example, the past 3 hours
>
> **Note 3 —** Selecting NONE in an operation drop-down menu clears the filter area of the associated column heading.
>
> **Note 4 —** Clicking on the Toggle Quick Filter button toggles the visibility of the filter areas on or off.
>
> **Note 5 —** The filter areas of the column headings are disabled if a filter was applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filter drop-down list. See Procedure 3-27 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 To refresh the search results using the currently defined filter, click on the Search button. If applied, the current filter is used even when the filter areas are hidden or closed.

6 Close the List Form.

Procedure 3-27 To perform an advanced search

1 Open a List Form.

2 Click on the Filter button at the top of the form. The filter window opens.

Note — The filter areas of the column headings in a List Form are disabled if a filter is applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filters drop-down list. See Procedure 3-26 for more information about performing a simple search using column headings.

3 Configure the filter properties.

- **i** Choose an item from the Attribute drop-down menu.
- **ii** Choose an item from the Function drop-down menu.
- **iii** Choose an item from the Value drop-down menu.
- **iv** Choose a Boolean Operator from the Operators drop-down menu.
- **v** Click on the Add button.

4 Do one of the following.

- **a** To filter additional properties, repeat step 3.
- **b** To modify the search filter, go to step 5.
- **c** If you are finished filtering properties, go to step 6.

5 Modify the search filter, if required.

- **a** Replace a Boolean operator.
  - **i** Select a Boolean operator in the summary area.
  - **ii** Choose an item from the Operators drop-down menu to replace the selected Boolean operator.

Note 1 — If an entire bracket is selected, all Boolean operators within are replaced at once.

Note 2 — If multiple filtered properties exist, replacing a Boolean operator wraps the properties associated with that operator in brackets.

b Exclude filtered properties.

i Select a filtered property in the summary area.

ii Click on the NOT button to exclude any matching entries from the search results.

Note 1 — If an entire bracket is selected, all filtered properties within are excluded at once.

Note 2 — Selecting an excluded property or a bracket and clicking on the NOT button includes the property or bracket again.

c Replace filtered properties.

i Select a filtered property in the summary area.

ii Configure the filter properties, as described in step 3.

iii Click on the Replace button.

d Delete filtered properties.

i Select a filtered property or a bracket in the summary area.

ii Click on the Delete button to remove the selected filtered properties from the search filter.

Note — Multiple filtered properties can be selected and deleted at once.

e Wrap filtered properties in brackets.

i Click the left mouse button and drag over multiple filtered properties in the summary area to select them.

ii Click on the brackets button to wrap the selected filtered properties in brackets.

Note 1 — Selecting properties that are already wrapped in brackets and clicking on the brackets button unwraps the selected properties.

Note 2 — Properties can only be wrapped or unwrapped if all Boolean operators contained within are matching.

6 Click on the Apply button or the OK button. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 3-28 To perform a search using the navigation tree

You can use the navigation tree to find specific objects. These objects include nodes, shelves, ports, and more.

1 Click on the Find... button on the navigation tree or press CTRL+F. The Find panel opens.

2 Configure the parameters as necessary. The parameters that are available for configuration vary depending on the view that has been selected.

3 Click on the Find button or press Enter. The first matching object is selected and expanded in the navigation tree.

4 To find additional matching objects, click on the Next button or press F3. The next matching object is selected and expanded in the navigation tree.

5 To return to the previous matching object in the navigation tree, click on the Previous button or press Shift+F3.

6 If required, click on the Clear button to clear all parameters configured in step 2.

7 Click on the Find... button or press CTRL+F to close the Find panel.

Procedure 3-29 To perform a search by specifying endpoints

Use the following procedure to find objects such as service tunnels, MPLS paths, VLAN paths and LSP paths by specifying endpoints.

1 Choose one of the following menu options from the 5620 SAM main menu:

- Manage→MPLS→Dynamic LSPs
- Manage→MPLS→Manual Bypass LSPs
- Manage→MPLS→Static LSPs
- Manage→MPLS→MPLS Paths
- Manage→MPLS→Static LSPs
- Manage→Service Tunnels
- Manage→VLAN→Paths

The Manage filter form opens.

2 Click on the Filter button. The filter window opens.

3 Choose Endpoints from the Select Filter Type drop-down menu. Endpoints is the default option.

Note — If a saved filter is selected or the filter areas of the column headings are populated, Advanced Filter is the default option.

4 Deselect the Any Source check box to pick a source IP address as a search filter. Otherwise, leave the Any Source check box selected to search by any source IP address.

5 Deselect the Any Destination check box to pick a destination IP address as a search filter. Otherwise, leave the Any Destination check box selected to search by any destination IP address.

6 Click on the Apply button. The results list is displayed based on the filter.

7 Click on the Close button to close the filter window.

8 Close the List Form.

Procedure 3-30 To locate an attribute on a configuration form

1 Open a configuration form.

2 Click on the Find button or press CTRL+F. The Find Attribute in list form opens and displays the attributes on the configuration form.

3 Configure the filter criteria and click on the Search button. A list of attributes is displayed.

4 Choose an attribute from the list and perform one of the following:

- a Click on the Show on Form button.
- b Double-click on the attribute row.
- c Press Enter.

On the configuration form, the selected name of the tab, panel, or field is highlighted and the associated tab is displayed.

Note — For configuration forms that can display multiple objects simultaneously, such as the service configuration forms, the search is performed only on the selected object.

Procedure 3-31 To filter object types

When an object drop-down list contains more than 10 items, you may click on the Filter for Object Type button to refine your search.

1 Open a List Form.

2 Click on the Filter for Object Type button. The Select Object Type form opens.

3 Configure the filter criteria using the filter area of any column headings.

Note — You can click on the Filter button on the Select Object Type form to open the filter window. See Procedure 3-27 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 Select an object from the list and click on the OK button. The Select Object Type form closes and the List Form reappears with the new Object Type selected in the Object Type drop-down.

Procedure 3-32 To filter using span of control

On some List Forms, you can create and save a span filter to display objects for your specific span of control. For example, if you only want to see objects within the span of control that has been assigned to you, create a span filter. You can also configure user preferences to automatically filter out objects that are not in your span of control.

1 Open a List Form.

2 If available, choose an entry from the object drop-down list.

3 Do one of the following.

 a To search using Span of Control from a List Form, go to step 4.

 b To search using Span of Control from the filter window, go to step 5.

4 Click on the Span On check box. The results list is displayed based on the filter. Go to step 9.

5 Click on the Filter button. The filter window opens.

6 Choose an entry from the Span drop-down list.

Note — An entry from the Span drop-down list is selected based on the Span On check box on the List Form.

7 Click on the Apply button. The results list is displayed based on the filter and the Span On check box is updated.

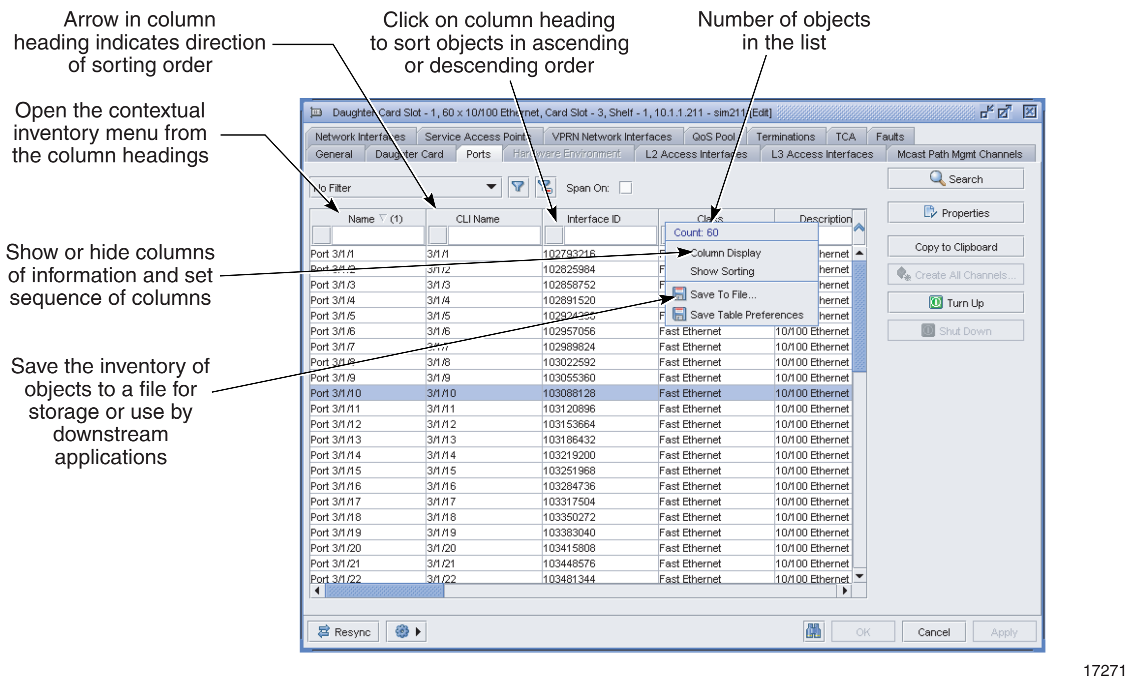
8 Click on the Close button. The filter window closes.

9 Close the List Form.

Procedure 3-33 To view and manage listed information

Many of the windows and forms are lists of network objects, for example, lists of ports displaying all the ports on a specific card. Figure 3-10 shows the major elements of a list.

Figure 3-10 List elements



On most lists, you can:

- generate inventories of the listed data
- reorganize the information from most important to least important

- remove columns of data that are not of interest
- sort listed information in ascending or descending order

1 Generate a list.

2 Perform an action on the list.

a To generate an inventory of data, right-click on the list heading. The Count indicates the number of objects in the list.

b To remove columns from the table:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the columns that you need to remove from the table and click the left arrow. The specified columns are moved to the Available for Table list box.

Note 1 — Columns that cannot be removed from the table are dimmed in the Displayed on Table list box.

Note 2 — There must be at least one column in a table.

iii To resequence the columns, go to step dii.

iv Perform one of the following.

- Click on the Apply button to apply the configuration changes without closing the form. The specified columns are removed from the table.
- Click on the OK button to apply the changes and close the Column Display window. The specified columns are removed from the table.
- Click on the Cancel button to close the Column Display window.

c To add columns to the table:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Available for Table list box, choose the columns that you need to add to the table and click the right arrow. The specified columns are moved to the Displayed on Table list box.

iii To resequence the columns, perform step dii.

iv Perform one of the following:

- Click on the Apply button to apply the configuration changes without closing the form. The added columns appear in the table.
- Click on the OK button to apply the changes and close the Column Display window. The added columns appear in the table.
- Click on the Cancel button to close the Column Display window.

d To reorganize the information:

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the name of the column that you need to move.

iii Click on the up and down arrows to move the column to the appropriate location in the table.

Note — You can move multiple columns simultaneously by choosing more than one column name before you click on the arrows.

iv Perform one of the following.

- Click on the Apply button to apply the configuration changes without closing the form. The columns appear on the table in the new sequence.
- Click on the OK button to apply the changes and close the Column Display window. The columns appear on the table in the new sequence.
- Click on the Cancel button to close the Column Display window.

Note — You can also resequence information by clicking on a column, dragging the column to the right or left, and dropping the column in the appropriate location.

e To sort data based on a column in ascending or descending order, click on the column heading. The down or up arrow changes and indicates the sequence in which the data is sorted.

f To sort data based on multiple columns, perform one of the following:

i Right-click on a column heading and choose Show Sorting from the contextual menu. The Show Sorting form opens. Choose the one or more properties from the Available for Sorting panel and click on the right arrow button. The properties appear in the Used for Sorting panel. Click on the Sort Ascending or Sort Descending, as required.

ii Click on the column heading of the first column by which you need to sort. Press and hold CTRL and click on one or more additional columns in the sequence in which you need to sort the data. The sort sequence appears in brackets after the column name. To change the direction of the sort, click on the heading of any of the selected columns while pressing CTRL.

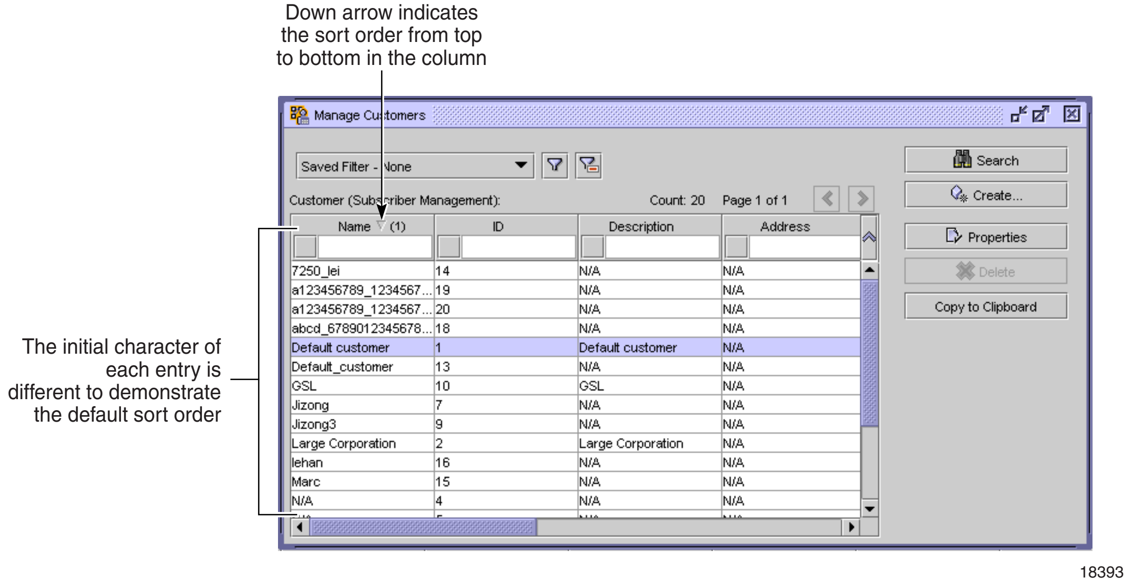
Note — To navigate quickly through a long sorted list, type a letter to move directly to the first item in the list that starts with that letter.

Table 3-7 describes the order in which different types of data are sorted from the top of the column to the bottom, based on the direction of the arrow in the column header. Figure 3-11 shows an example of information sorted in a column according to the down arrow in the column header.

Table 3-7 Sorting listed information

Entry type	Down arrow	Up arrow
Numbers only	Sorted from the lowest number to the highest number	Sorted from the highest number to the lowest number
Letters	Sorted left to right, character by character, in alphabetical order.	Sorted left to right, character by character, in reverse alphabetical order.
Alphanumeric	Sorted left to right, character by character, in the following order: from 0 to 9, then in alphabetical order	Sorted left to right, character by character, in the following order: in reverse alphabetical order, then from 9 to 0
Special characters	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: (space) ! # $ % & ‘ ( ) * + , . / The following characters are sorted in the following order after numbers in a list, but before uppercase and lowercase letters: : ; < = > ? @ The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: { | } ~	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: ~ } | { The following characters are sorted in the following order before numbers in a list, but after uppercase and lowercase letters: @ ? > = < ; : The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: / . , + *) (‘ & % $ # ! (space)
Blanks	Blank entries are placed first at the top of the list.	Blank entries are placed last at the bottom of the list.

Figure 3-11 List sort order example



Procedure 3-34 To save listed information to a file

After you list information, as described in Procedure 3-33, you can save a copy of the list for purposes such as the following:

- record keeping
- inventory management
- processing by another application

1 Generate a filtered list, as required.

2 Right-click on a list column heading and choose Save To File from the contextual menu. The Save As form opens.

Note — The 5620 SAM uses the user home directory as the default location for saved files.

3 Use the form to specify the name and location of the file that is to contain the listed information. You can save the information in the following formats:

- plain text
- HTML
- CSV

4 Click on the Save button. The information is saved as specified and the Save as form closes.

Procedure 3-35 To configure the maximum number of objects on a list form

Perform this procedure to specify the maximum number of objects to display per page on a list form.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Configure the Specify # of Items Per Page parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 3-36 To save results list preferences

You can save results list preferences, so when similar searches on similar objects are performed, the output of the list is organized according to your preferences.

1 Open a List Form.

2 Organize the results list according to preference, for example, whether to sort columns of data in ascending or descending order.

3 Right-click on a results list column heading and choose Save Table Preferences from the contextual menu. A dialog box appears to confirm that you want to save the current filter preferences.

Note — Choosing Save Table Preferences from a contextual menu does not save any filter configurations.

4 Click on the Yes button. The results list format is saved.

Each time a similar list is generated for similar objects, for example, if you configured a table preference for generating lists of ports, then each time you list ports, results are displayed according to preconfigured table formats.

5 Close the List Form.

Procedure 3-37 To save search filters

List Forms allow you to save filters for object types. The filters created only apply to the specific object type against which the filter is created and saved, and that object type's descendant objects.

1 Open a List Form

2 Define filter properties, as described in Procedure 3-26 and click on the Filter button, or define filter properties, as described in Procedure 3-27. The filter form opens.

3 Click on the Save... button. The Save Filter form opens.

4 Configure the parameters:

- Filter Name
- Description
- Public

Note — These parameters have pre-populated values when a saved search filter is loaded or selected from the saved filters drop-down list, or if the filter was previously saved.

5 Click on the Save button. The Save Filter form closes. The defined filter is saved for a future search on a similar object type and the configured parameters are populated in the filter window.

6 Click on the Apply button of the OK button to use the filter. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 3-38 To clear a search filter

Use the following procedure to clear search filters from a List Form or the filter window.

1 Open a List Form.

2 Define filter properties as described in Procedure 3-26 or 3-27.

3 Do one of the following.

a To clear all search filters from a List form, go to step 4.

b To clear the search filter of the filter window, go to step 7.

4 Do one of the following.

a Click on the Clear all Filters button. Any filtered properties are cleared.

Note — Clicking on the Clear all Filters button does not clear or refresh search results.

b Choose No Filter from the saved filters drop-down list. Any filtered properties are cleared and the results list is displayed based on the empty filter. Go to step 11.

5 Click on the Search button. The results list is displayed based on the empty filter.

6 Go to step 11.

7 Click on the Filter button. The filter window opens.

8 Click on the Clear button. Any filtered properties are cleared from the filter window.

9 Click on the Apply button or the OK button. The results list is displayed based on the empty filter.

10 If the filter window is open, click on the Close button. The filter window closes.

11 Close the List Form.

Procedure 3-39 To load a saved search filter

Use the following procedure to load search filters from a List Form or the filter window. See Procedure 5-22 for information about loading a saved filter on a topology map.

1 Open a List Form.

2 Do one of the following.

a To load search filters from a List Form, go to step 3.

b To load search filters from the filter window, go to step 4.

3 Choose an entry from the saved filters drop-down list. The results list is displayed based on the filter. Go to step 11.

Note 1 — Choosing an entry from the saved filters drop-down list disables the filter areas of the column headings.

Note 2 — Only saved filters that are applicable to the current object type and its ancestor types appear in the saved filters drop-down list.

Note 3 — Selecting None from the saved filters drop-down list clears any filtered properties on the current form and immediately refresh the results list.

Note 4 — The contents of the filter window are updated based on the entry selected from the saved filters drop-down list.

4 Click on the Filter button. The filter window opens.

5 Click on the Saved Filters button. The Saved Filters window opens and displays filters that have been saved for the current object type and its ancestor type(s).

6 Select a saved filter in the list.

7 Click on the Load button. All the properties of the filter window are replaced with the contents of the saved filter.

8 If desired, modify the filter and click on the Save button to save it.

Note — The filter is saved using the current object type, regardless of the object type of the saved filter that was loaded.

9 Click on the Apply button or the OK button to use the filter. The results list is displayed based on the filter.

10 If the filter window is open, click on the Close button to close the filter window.

11 Close the List Form.

Procedure 3-40 To delete a saved search filter

Use the following procedure to delete saved search filters from the filter window.

1 Open a List Form.

2 Click on the Filter button. The filter window opens.

3 Click on the Saved Filters button. The Saved Filters window opens.

4 Select a saved filter in the list.

5 Click on the Delete button. The filter is deleted.

6 Close the form.

7 Close the filter window.

8 Close the List Form.

Procedure 3-41 To create equipment group search filters

On some list forms you can create and save search filters based on pre-existing topology groups.

1 Open a list form, if available, choose an entry from the object drop-down list. The equipment group filter drop-down list displays with Equipment Group(s) - All selected.

2 Choose Select Equipment Groups from the equipment group drop-down list. The Select Equipment Groups window appears with the topology groups listed in the Available column. See Procedure 5-29 for information about how to create a topology group.

3 Perform one of the following:

a To create an equipment group filter.

i In the Available list box, choose the topology groups that you need to include in the filter and click on the right arrow. The specified topology groups are moved to the Filtered by list box.

ii To include data from nodes that are in equipment subgroups in the equipment group filter, select the Include contained Equipment Groups check box.

iii Go to step c.

b To modify an equipment group filter.

i Click on the Saved Filters button. The Save Filter form displays the equipment group filters.

ii Select a filter and click on the Load button. The Save Filter form closes and the selected filter is displayed in the Select Equipment Groups window.

iii Update the selected equipment group filter as required.

iv Go to step c.

c To save an equipment group filter.

i Click on the Save button. The Save Equipment Group Filter displays.

ii Configure the parameters:

- Filter Name
- Description
- Public

Note — The parameters have pre-populated values when a saved equipment group filter is loaded or is selected from the saved filters drop-down list, or if the filter was previously saved.

iii Click the Save button. The Save Equipment Group Filter form closes, the filter is saved, and the Select Equipment Groups window displays the saved equipment group filter.

d Click on the Clear button to clear the current filter from the Select Equipment Groups window.

4 Click on the OK button to apply the filter without saving it. The results list is displayed based on the equipment group filter and any additional filters that are applied to the list. The Last Search value is updated, and the equipment group filter name is displayed in the equipment group filter drop-down list.

5 Close the list form.

Procedure 3-42 To perform a search using equipment group filters

On some list forms, you can create and save a filter based on pre-existing topology groups.

1 Open a list form, if available, choose an entry from the object drop-down list. The equipment group filter drop-down list displays with Equipment Group(s) - All selected.

2 Choose a filter from the equipment group drop-down list. The results list is displayed based on the selected equipment group filter and any additional filters that are applied to the list. The Last Search value is updated.

3 Close the list form.

4 — 5620 SAM navigation tree overview

4.1 Navigation tree overview

The navigation tree lists the managed equipment, services, and protocols that are configured on the NE. The navigation tree includes a view selector located on the navigation tree toolbar. The view selector is a drop-down menu that lists the physical and logical network views that are available.

The navigation tree is accessible from the main window, configuration forms, and maps.

You can choose the following views:

- Equipment—displays the physical objects that the 5620 SAM manages
- OSPF—displays the OSPF objects in the network
- IS-IS—displays the OSPF objects in the network
- Routing—displays the device routing instances and child objects such as the network interfaces and the configured protocols
- Ring Group—displays the ring group objects that the 5620 SAM manages

Table 4-1 describes the objects in the equipment view of the navigation tree that the 5620 SAM allows you to create and manage.

Note — The device properties forms include a navigation tree that is displayed on the left of the form. The root of the device properties form navigation tree is the device.

Table 4-1 5620 SAM navigation tree object descriptions — Equipment view

Object	Description
Routing	The network — contains the routers, devices, and topology groups, including the default Discovered NEs and Unmanaged NEs topology groups
Router, device, topology group	The second level in the hierarchy
CCAG, ISA-AA groups, ISA-Tunnel groups, ISA-LNS groups, ISA-NAT groups, ISA-Video groups, LAG, IGH, shelf	The third level in the hierarchy
APS groups	Located under the shelf object; contain the APS groups for a device
Card	Located under the shelf object
Daughter card	A child object of the card object
Bundles	A child object of the daughter-card object; a group of DS0 channels on a SONET- or TDM-capable daughter card
Port	A child object of the daughter-card object
Channel, sub-channel, timeslot	Child objects of the port object
Fans	Located under the shelf object[1]
Power Supplies	Located under the shelf object[1]

Note
(1) This object is not supported on 1830 PSS nodes.

You can use the following methods to view and manage objects in the 5620 SAM navigation tree:

- Double-click on an object or press the + key when the object is selected to open the object and to display the child objects.
- Double-click on an object or press the - key when the object is selected to close the object and to hide the child objects. A + key to the left of the map object indicates that the object contains child objects. For example, a topology group that contains one or more child topology groups has a + key to the left of the topology group in the navigation tree.
- Click on an object and use the cursor keys to navigate the object hierarchy. In the Equipment view, for example, you can navigate from the device to the ports and channels.
- Right-click on an object to open the contextual menu and choose a function. The menu options are specific to the object type. See "Contextual menus" in this section for more information.

Note — Keyboard-based navigation-tree operations may not function as expected when you open the client GUI using a third-party access tool, for example, a Citrix server.

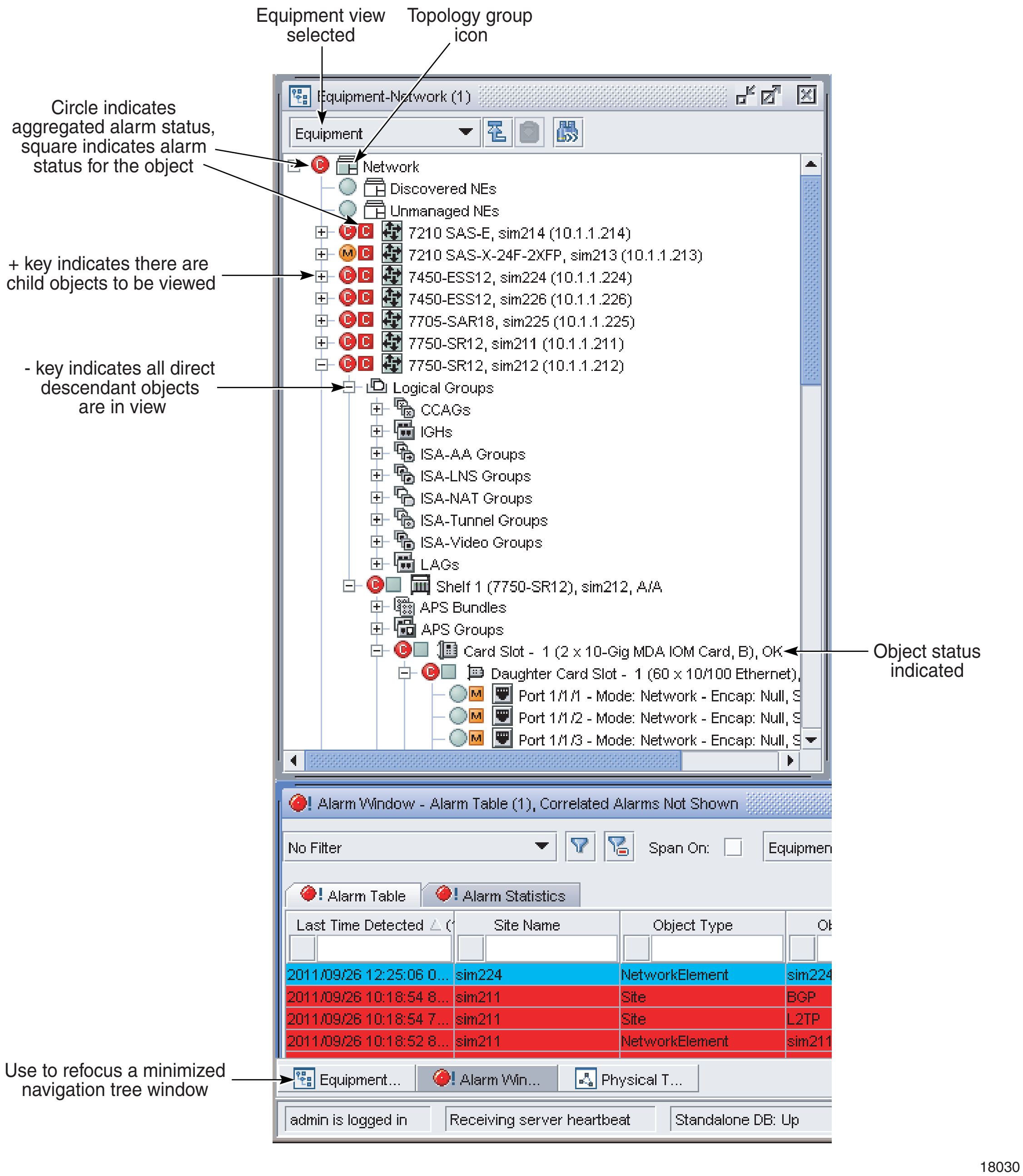
The navigation tree uses color highlights to display object status information such as the current alarm level and the aggregated alarm status. The operational and administrative states of an object are displayed in text form beside the object icon, as are the object type and description.

The circle icon to the left of the topology group icon represents the aggregated alarm status for the group. It represents the most serious alarm against descendant device.

The topology group icon is divided into three sections. The top right square represents the most severe state of all descendant devices. The bottom right square represents the most severe state of all descendant links. The bottom section of the topology group icon represents the most severe state of the devices and edges that are immediately descendant of the group. See chapter 37 for more information about viewing alarm status information in a map navigation tree. To troubleshoot alarms using topology maps, see *5620 SAM Troubleshooting Guide*.

Figure 4-1 shows some of the navigation tree objects that you can manage using the Equipment view.

Figure 4-1 5620 SAM navigation tree objects - Equipment view



Using the navigation tree toolbar

The navigation tree toolbar consists of the view selector, the Make Root At Top Level button, and the Copy to Clipboard button. Figure 3-1 shows the navigation tree toolbar. See Procedure 3-24 for information about using the Copy to Clipboard button.

Make Root At Top Level button

The Make Root At Top Level button restores the navigation tree to the default root. For example, in the equipment view, if you redefine the root of the tree as a card and click on the Make Root At Top Level button, the navigation tree refreshes with the default root, which is the network. The Make Root At Top Level button is enabled only when the root is not the network. The Make Root At Top Level button is available only for the equipment view.

Make Root and Make Root In New Tree menu options

The navigation tree contextual menus provide Make Root and Make Root In New Tree menu options that allow you to redefine the root of the tree. These menu options, along with the Make Root At Top Level button, help orient users in densely populated navigation trees. The menu options are available only for the equipment view. See “Contextual menus” in this section for more information about using these functions.

Copy to Clipboard button and Clipboard window

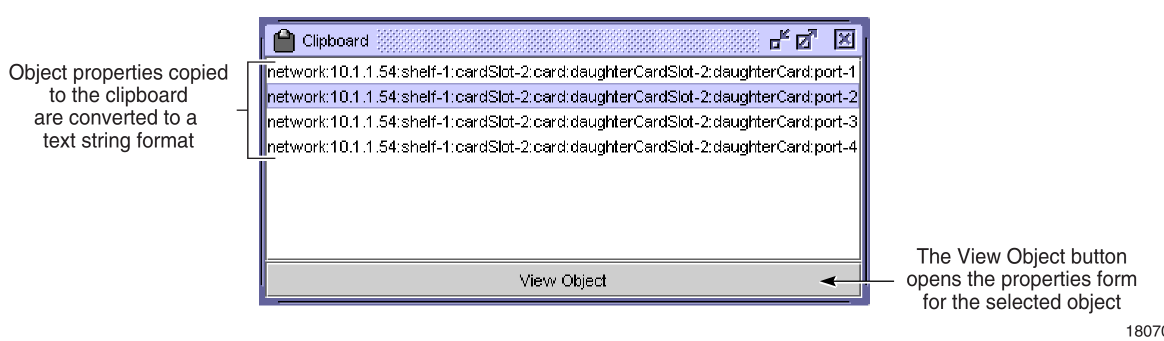
Using the Copy to Clipboard button on the navigation tree toolbar, you can copy the identifier of one or more 5620 SAM objects to the Clipboard window. You can then open the Clipboard window from the Application menu to retrieve the identifier and paste it into another application. You can also choose an object identifier in the Clipboard window and click on the View Object button to open the object properties form. The elements in an object identifier are delimited using colons (:).

The Copy to Clipboard button is on list forms and on the list tabs of properties forms. You can use the button to copy configurable and read-only text fields. The button is enabled when at least one object is selected.

Note — The Clipboard window keeps the object identifier from only the most recent copy action. After you copy an object identifier to the clipboard, if you click on the Copy to Clipboard button again to copy another object identifier, the second copy action overwrites the previously copied identifier in the Clipboard window.

Figure 4-2 shows the Clipboard window. See Procedure 3-24 for more information about using the clipboard function.

Figure 4-2 Clipboard window



Paste from Clipboard button

After using the Copy to Clipboard button to copy object identifiers to the Clipboard window, you can use the Paste from Clipboard button on the physical link properties form to set multiple parameters at one time using the copied object identifiers. See Procedure 5-34 for information about using the Paste from Clipboard button.

Contextual menus

Each object in the 5620 SAM navigation tree has a contextual menu that opens when you right-click on the object. Contextual menus are also accessible when you right-click on map objects.

You can use the contextual menus to do the following:

- create objects
- configure object properties
- perform maintenance functions
- change the state of objects
- open a different management interface, for example, a CLI
- designate an object as the root object in the navigation tree

The contextual menu options are specific to the object type. Table 4-2 lists the contextual menu options in alphabetical order.

Warning — In a composite service, deleting a service is not the same as removing a service from a composite service. Deleting a service removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking.

See Procedure 76-4 for more information about removing a service from a composite service.

Table 4-2 Contextual menu options

Option name	Description
Add to Ring Group	The Add to Ring Group menu option specifies whether to add the device to a group.
Configure Card	The Configure Card option opens the Create Card properties form that allows you to create a card configuration for the slot. You assign a supported card type to the slot. The options available are displayed with check marks beside them in the Supported Card Types parameter. The Equipped Card Type displays the card type that is physically in the slot. When the configured card types are correct, you can change the Administrative State as required.

(1 of 6)

Option name	Description
Configure Daughter Card	The Configure Daughter Card option opens the Daughter Card (Create) form that allows you to create a daughter card configuration for the slot. You assign a supported daughter card type to the daughter card slot. The options are displayed with check marks beside them in the Supported Daughter Card Types area of the form. The Equipped Daughter Card Type displays the daughter card type that is physically in the slot. When the configured card types are correct, you can change the Administrative State as required.
Copy to Clipboard	The Copy to Clipboard option copies the MDA information to the clipboard.
Create All Channels	The Create All Channels option allows you to automatically create all of the channels on ports with available channels. This option is available for OC12, OC3, and DS3 and E3 ASAP, APS and MC-APS ports.
Create APS Group	The Create APS Group menu option opens the APS Group (Create) form that allows you to create and manage APS groups on the shelf.
Create APS Protection Bundle	The Create APS Protection Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS protection bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
Create APS Protection Channel	The Create APS Protection Channel menu option opens the APS Channel, Protection (Create) form that allows you to create and manage APS protection channels.
Create APS SONET Channel	The Create APS SONET Channel menu option opens the SONET Channel (Create) form that allows you to create the APS common configuration.
Create APS Working Bundle	The Create APS Working Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS working bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
Create APS Working Channel	The Create APS Working Channel menu option opens the APS Channel, Working (Create) form that allows you to create and manage APS working channels.
Create Bundle Members	The Create Bundle Members option opens the Add Bundle Member form, which allows you to add members to an APS bundle or a multilink bundle.
Create Bundle	The Create Bundle option opens the APS Bundle Display configuration form or the the Create Multilink Bundle configuration form, which allows you to create a group of DS0 channel groups on a channelization-capable MDA. You configure bundle parameters and add bundle members. When the Create Bundle option is used to open the APS Bundle Display configuration form, the DS0 channel groups that you create provide bi-directional APS protection on IMA bundles. When the Create Bundle option is used to open the Create Multilink Bundle configuration form, the DS0 channel groups that you create provide a mechanism to distribute data across multiple links to achieve higher bandwidth on a SAP. You can create IMA group bundles on channelized ASAP MDAs.
Create CCAG	The Create CCAG option opens the CCAG (Create) form, which allows you to create a cross-connect aggregation group. You define CCAG properties, configure CCAG parameters, and configure CCAG members.

(2 of 6)

Option name	Description
Create Channel	The Create Channel option allows you to create channels on ports with available channels.
Create Group	The Create Group contextual menu option opens the Group (Create) form to create a topology group in the equipment view of the navigation tree and on the appropriate topology maps.
Create IGH Members	The Create IGH Members option opens the Create IGH Member configuration form which allows you to configure IGH member ports.
Create IGH	The Create IGH option opens the IGH (Create) form, which allows you to create an IGH. You define IGH properties, and configure IGH subgroups and members.
Create Interface	The Create Interface option is available for CES ports on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA. This option allows you to create an interface for a TDM line, such as E1 or T1, for backhauling the TDM signal through the IP/MPLS network.
Create ISA-AA Group	The Create ISA-AA Group option opens the ISA-AA Group (Create) form, which allows you to create an ISA-AA group and ISA-AA partitions. You define ISA-AA group and ISA-AA partition properties, configure ISA-AA group and ISA-AA partition parameters, and specify ISA-AA members.
Create ISA-Tunnel Group	The Create ISA-Tunnel Group option opens the ISA-Tunnel Group (Create) form, which allows you to create an ISA-Tunnel group. You define ISA-IPsec properties, configure ISA-IPsec parameters, and specify ISA-IPsec members.
Create ISA-LNS Group	The Create ISA-LNS Group option opens the ISA-LNS Group (Create) form, which allows you to create an ISA-LNS group. You define ISA-LNS properties, configure ISA-LNS parameters, and specify ISA-LNS group members.
Create ISA-NAT Group	The Create ISA-NAT Group option opens the ISA-NAT Group (Create) form, which allows you to create an ISA-NAT group. You define ISA-NAT properties, configure ISA-NAT parameters, and specify ISA-NAT group members.
Create ISA-Video Group	The Create ISA-Video Group option opens the ISA Video Group (Create) form, which allows you to create an ISA-Video group. You define ISA-Video properties, configure ISA-Video parameters, and specify ISA-Video group members.
Create LAG Members	The Create LAG Members option opens the Create LAG Member configuration form where you define LAG member ports.
Create LAG	The Create LAG option opens the Create LAG configuration form. You define LAG properties, configure LAG parameters, configure LAG subgroups and members, and configure LACP.
Create Ring Group	The contextual menu option for a network is Create Ring Group, which is used to group devices to be able to create VLAN or VPLS ring groups.

(3 of 6)

Option name	Description
Delete	For daughter cards, bundles, ports, and channels, the Delete option deletes the selected object when the object and everything contained in the object is set to administratively down. For topology groups, and IGH groups, the Delete option deletes the selected group object once all objects in the group have been removed from the group. For SC APS Bundle objects, the Delete option deletes the APS common configuration from the APS group. For all other objects where the Delete option is available, the Delete option deletes the object and all contained objects from the network. This option is not available for the network (root) topology group.
Discovery Manager	The Discovery Manager option opens the Discovery Manager (Edit) form. You can create NE discovery rules and discover NEs. See chapter 14 for information about discovering NEs and creating discovery rules.
Duplicate Links	On the physical topology map, the Duplicate Links option displays a fly-out menu. You can choose either the Highlight Duplicate Links or Delete Duplicate Links option. It is possible for both a manual link and a discovered physical link to exist on the same two endpoints. When this happens, a duplicate link alarm is raised. This alarm only occurs on point-to-point links and when both endpoints are ports or LAGS. You can identify such duplicate links by choosing the Highlight Duplicate Links option. You can remove these duplicate links by choosing the Delete Duplicate Links option. This action prompts you with a warning and then delete all of the manually created physical links. This alarm is not raised on existing manual links (for example, those in place after a database upgrade).
Equipment	The Equipment option opens a Group (Create) form to create a descendant topology group for the selected group in the navigation tree. For physical topology maps, you can also choose the Create Physical Link option to create links between map objects.
Force Mode	The Force Mode menu option forces an upgrade of the hardware.
Highlight MTU Mismatch	The Highlight MTU Mismatch option is used to highlight MTU mismatches between physical ports. When the configured MTU on two or more endpoints do not match, an alarm is raised to notify the operator of a possible configuration error. This is supported on both point-to-point and broadcast physical links. MTU mismatches can also be discovered by conducting an RCA audit. See Procedure 81-6 for more information.
Highlight Nearest Customer Links	The Highlight Nearest Customer Links option is used to highlight the nearest customer links between nodes. See “LLDP” in chapter 30 for more information.
Highlight Nearest Non-TPMR Links	The Highlight Nearest Non-TPMR Links option is used to highlight the nearest Non-Two Port MAC Relay links between nodes. See “LLDP” in chapter 30 for more information.
Highlight Upper Layer Adjacency Links	The Highlight Upper Layer Adjacency Links option is used to display hidden links between nodes.
List	The List option opens the Discovered NEs form with a list of newly discovered NEs or the Unmanaged NEs form with a list of newly added Unmanaged NEs.

(4 of 6)

Option name	Description
Make Flat Map for Group	The Make Flat Map for Group option opens a flat map of the topology group.
Make Root	The Make Root option makes the selected object the root of the navigation tree. The default root is the network.
Make Root In New Tree	The Make Root In New Tree option opens another navigation tree window with the selected object as the root of the tree.
NE Sessions	The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device in the equipment view of the navigation tree.
Open URL	The Open URL option opens the Web browser to manage the GNE.
Properties	The Properties option opens the property form for the selected object. This form allows you to view read-only information and to configure parameters associated with the selected object. If the Copy button is available, you can use the Copy button to create topology groups in the network using the same parameter information.
Reboot	The Reboot option specifies that all cards in the chassis are re-initialized.
Reference	The Reference option displays a fly-out menu. You can choose from the Set All, Clear All, or the Cleanup All options. • The Reference option essentially takes a snapshot of the physically topology at a specific time. Any deviation from this checkpoint can then be subsequently shown. • The Set All option checkpoints all currently discovered links that exist. Any object that was previously checkpointed and is operationally down is left untouched. Any object that goes operationally down in the future is not removed, but is simply marked as operationally down. • The Clear All option clears all object checkpoints. Any object that is operationally down (shown as a red link) is removed from the database. Any non-checkpointed object that becomes operationally down in the future is removed from the system. • The Cleanup All option keep the current checkpoint set for objects that are operationally up, but removes checkpoints from objects that are operationally down objects. This is basically the same as the Clear All option, but only affects operationally down objects.
Remove	The Remove option deletes the service from the network in a composite service tier. See Warning note above.
Remove Card	The Remove Card option deletes the card from the slot when the slot and everything contained in the slot is changed to administratively down.
Remove From Ring Group	The Remove From Ring Group option removes the specified device from the ring group. The devices are not deleted; they remain in the equipment view of the navigation tree.
Remove Ring Group	The Remove Ring Group option removes the specified ring group. The devices contained in the ring group are not deleted; they remain in the equipment view of the navigation tree.
Resync	The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.

(5 of 6)

Option name	Description
Scripts	The Scripts option is available to users with the appropriate scope of command roles. This option allows you to associate scripts and templates to object types directly from the navigation tree or from map objects without having to navigate through the Script Manager. The Scripts option displays a fly-out menu. You can choose from the Add Script and Manage Scripts option. Associated scripts and templates are also displayed on the fly-out menu. The type of script or template is identified by the icon located to the left of the script or template name. • The Add Script option opens the Select Script(s) window. From this window you can associate existing scripts and templates to the selected object type. You can also edit and create scripts and templates from the Select Script(s) window. • The Manage Scripts option allows you to add and remove script and template associations with the selected object type. You can also access the Scripts option from the configuration form.[(1)] See the *5620 SAM Scripts and Templates Developer Guide* for more information about the Script Manager.
Shut Down	The Shut Down option specifies that the selected object is changed to administratively down.
Shut Down MC LAG	The Shut Down MC LAG option specifies that the MC LAG is changed to administratively down.
Shut Down Peer	The Shut Down Peer option specifies that the MC peer is changed to administratively down.
Soft Reset	The Soft Reset option resets the card. A soft reset is preferable to a reboot, as it results in minimal downtime. A soft reset causes the card to stop all processes it is running and restart.
Turn Up MC LAG	The Turn Up MC LAG option specifies that the MC LAG is changed to administratively up.
Turn Up Peer	The Turn Up Peer option specifies that the MC peer is changed to administratively up.
Turn Up	The Turn Up option specifies that the selected object is changed to administratively up.

(6 of 6)

Note

(1) The Scripts option may be located under the More Actions button if more than one option exists for the configuration form.

4.2 Basic navigation tree procedures

Use the following procedures to manage equipment using the navigation tree.

Procedure 4-1 To make a selected object the root of the navigation tree

Use the Make Root option of the contextual menu to make a selected object the root of the navigation tree. The Make Root option is only available in the Equipment view. See section 4.1 for information about the navigation tree objects that support the menu option.

The Make Root option of the contextual menu is not available for an object that is positioned one object level below the root of the tree. For example, in a navigation tree where the device is the root of the tree, the LAG object and the shelf object do not support the Make Root option.

Right-click on the navigation tree object that you want to make the root of the tree and choose Make Root from the contextual menu. The navigation tree is refreshed with the selected object as the root of the tree. The Make Root At Top Level button is enabled.

See Procedure 4-3 for information about restoring the default root of the navigation tree.

Procedure 4-2 To make a selected object the root of another navigation tree

Use the Make Root In New Tree option of the contextual menu to make a selected object the root of another navigation tree.

Note — Up to seven navigation tree windows can be open at the same time and each tree must have a different root when it is first created.

The Make Root In New Tree menu option is only available in the equipment view. The Make Root In New Tree option is not available in the contextual menu for the root object of a tree. See section 4.1 for information about the navigation tree objects that support the menu option.

Right-click on the navigation tree object that you want to make the root of another navigation tree and choose Make Root In New Tree from the contextual menu. Another navigation tree window appears with the selected object as the root of the tree.

Procedure 4-3 To restore the default navigation tree root

The default root of the navigation tree is the network object. When the root is not the network object, the Make Root At Top Level button is enabled.

Click on the Make Root At Top Level button in the navigation tree toolbar to restore the default root of the tree. See section 3.1 for more information about the Make Root At Top Level button.

5 — 5620 SAM map management

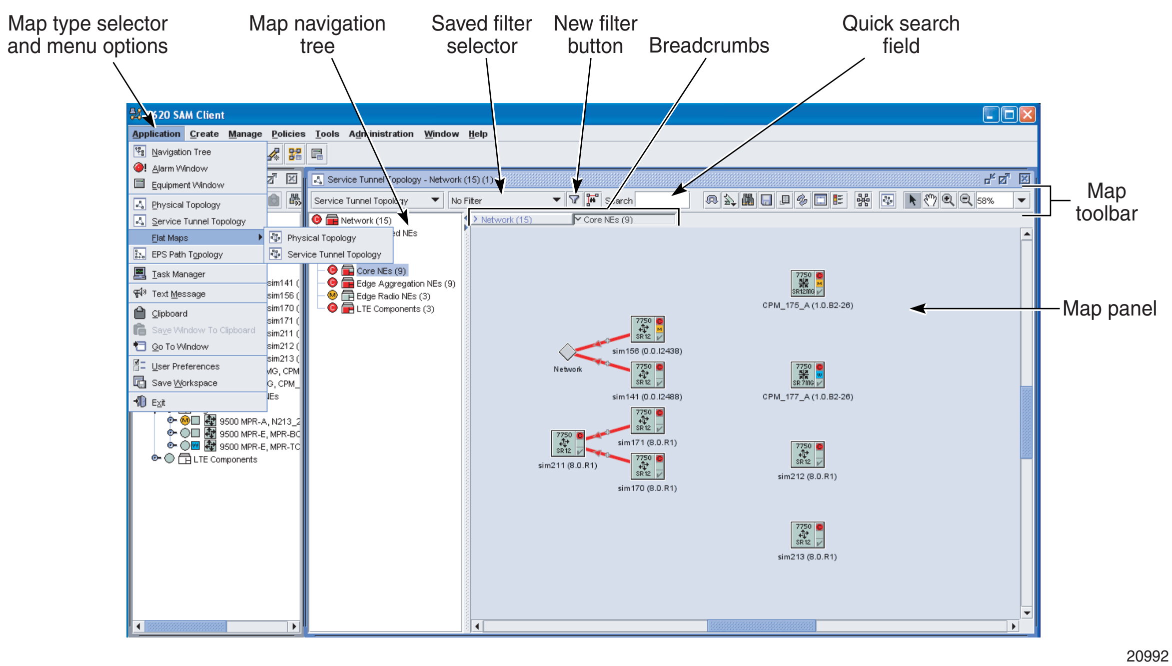
5.1 5620 SAM map management overview

The following 5620 SAM network topology maps are available:

- physical
- service tunnel
- service
- composite service
- LSP path
- LSP cross-connect

Each map displays network objects and information, and provides contextual menus to open forms that display additional information. In the context of a 5620 SAM map, a link object, such as a physical link or service tunnel, is called an edge. An object other than a link between objects, such as an NE or a topology group, is called a vertex. Figure 5-1 shows the main map elements.

Figure 5-1 Map elements



Map window

The map window includes the following:

- a title bar
- a map panel that displays the network objects
- a navigation tree that lists the topology groups
- a toolbar, which consists of a view selector, saved filter selector, quick-search field, and buttons that perform various functions

The title bar of the map window displays the following information:

- map type, for example, Physical Topology
- path from the network root to the currently displayed topology group; each step in the path is called a breadcrumb
- map number, for example, the first or the tenth map opened

Map panel

The map panel is associated logically with the map navigation tree. As the user navigates through the topology groups in the map navigation tree, the contents displayed on the map panel change. The topology group that is selected in the map navigation tree is the group that is displayed on the map panel.

When you double-click on a topology group object, the contents of the group on the map panel are displayed and the group is selected and opened in the map navigation tree. When you double-click on other map objects, such as routers or links, their property form opens. Right-click on any map object to display a contextual menu.

When map objects are linked between different topology groups, the line representing the connection terminates on a map object called a connector. The connector indicates that the endpoint of the link resides in another topology group. The label of the connector icon is the name of the topology group to which the link points. Connector objects do not have contextual menus.

When a physical link is created between a port or LAG managed by the 5620 SAM and an unmanaged object, the unmanaged object is called a remote endpoint. The remote endpoint label is configured by the user when the physical link is created.

You can configure a background image to display in the map panel for a topology group, for example, a map image of North America. You can position device icons and topology group icons in the map of the network to reflect their relative geographic locations.

Selecting map objects

Click on the Select Tool button to select an object on the map. You can select multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all of the objects you want to select on the topology map. You can also press CTRL-A to select all items on a map.

You can select one or more objects and view them exclusively in a map by right-clicking on the selection and choosing Show Only Selected. The map is then filtered to display only the selected objects and the links between them. Links to other objects are not shown. You can revert to the previous view by right-clicking in the map and choosing Cancel Show Only.

When multiple objects are selected, you can shift the map focus to the next object using the F3 key, and shift the map focus to the previous object by pressing CTRL-F3.

You can also select all of the NEs that are attached to an NE by selecting one or more NE and right-clicking and choosing Select Attached.

You can deselect a selected NE by pressing the CTRL key and clicking on the NE.

Moving map objects

The 5620 SAM allows you to move map objects in the following ways:

- in the map panel; for example, to add a router to a topology group by dragging and dropping the router object to the topology group object in the map panel
- from the map panel to the map navigation tree; for example, to add a router to a topology group by dragging and dropping the router object from the map panel to the topology group object on the map navigation tree
- after discovery by using either the or by moving the tiled icons to a new map panel location
- between two maps
- in the map navigation tree; for example, to make a topology group the immediate descendant of another topology group by dragging and dropping one topology group object to another topology group object in the map navigation tree

When a topology group is created, users with Topology Mgmt privileges can populate the group from the topology map by dragging and dropping map objects into the group in the map panel or in the map navigation tree, or from the map panel to the map navigation tree.

Note — You cannot move map objects to or from groups that are not within your span of control.

By default, users can move map objects and change the layout of the objects on the map, however the changes are not saved to the database when the map is closed. The ability to save changes to the layout of topology maps is controlled by scope of command roles and access permissions. Permissions are set by using 5620 SAM security configuration forms. See chapter 9 for more information about setting access privileges.

The Reload button icon indicates when you move a map object and change the layout of the objects. The Reload button icon changes to indicate whether moving a map object and changing the layout of the objects is saved to the database. See “Map toolbar” in this section for more information about the Reload button.

Note — When you move a map object in the map panel, the X,Y coordinates for the map object change. If you have update and execute scope of command access permission, this change affects all users that display the map view and the topology group.

Connectors can only be moved in the map panel. Connectors cannot be moved to another topology group.

Finding map objects quickly

The Search field beside the toolbar buttons is used to quickly locate a map object. When you enter a text string in the Search field and press ↵, the 5620 SAM searches each object name in the map for the string. If a match is found, the map focus shifts to the object. If multiple matches are found, you can shift the map focus to the next object using the F3 key, and shift the map focus to the previous object by pressing CTRL-F3.

Links and link groups

The topology maps display single links and multiple links that connect two map objects. Links are used to represent the physical connectivity between two NEs or logical connectivity, such as service tunnels. The map uses an arrow to display the direction of a unidirectional link. Multiple links between 2 objects are grouped, by default, as one link with no defined direction. Bidirectional links are displayed with no defined direction. A link group is displayed with a plus sign located on the link object.

When you double-click on a single link, the properties form for the link opens. When you double-click on the link group object for multiple links, a list form opens displaying all of the links that belong to the link group. For the physical, service tunnel, and LSP maps, a list form opens regardless of whether there is one link or multiple links in the link group.

A bidirectional link group is displayed with a plus sign icon located in the middle of the link object. A unidirectional link or link group is displayed using an arrow icon on the object pointing in the direction of the path.

The color of a single link object is determined by the status of each link endpoint. The color of a link group object is determined by the most serious alarm that is raised for a link in the link group.

Breadcrumbs

Breadcrumbs are buttons that are displayed along the top of the map panel. Breadcrumbs indicate, from left to right, the hierarchy of the topology groups to the group currently displayed in the map panel. The default top of the hierarchy, the breadcrumb at far left, is the entire network. Click on a breadcrumb to open the map for the corresponding group.

Map navigation tree

The following network topology maps display a map navigation tree:

- physical map
- service tunnel map

You can use the map navigation tree:

- for non-linear navigation to any topology group on the map
- to display the topology group hierarchy starting from the entire network

The map navigation tree displays:

- topology groups, including group names
- status of the topology groups

When you click on a map object in the map navigation tree, the contents of the object are displayed in the map panel, and the map object is selected. See section 4.1 for more information about the navigation tree.

Contextual menus for objects in the map navigation tree

To open a contextual menu for an object, right-click on a map object in the map navigation tree. See Table 4-2 for more information about contextual menu options.

Map toolbar

The map toolbar allows you to manage a 5620 SAM map view. The toolbar is above the map panel in the map window. Figure 5-2 shows the map toolbar elements.

Figure 5-2 Map toolbar elements

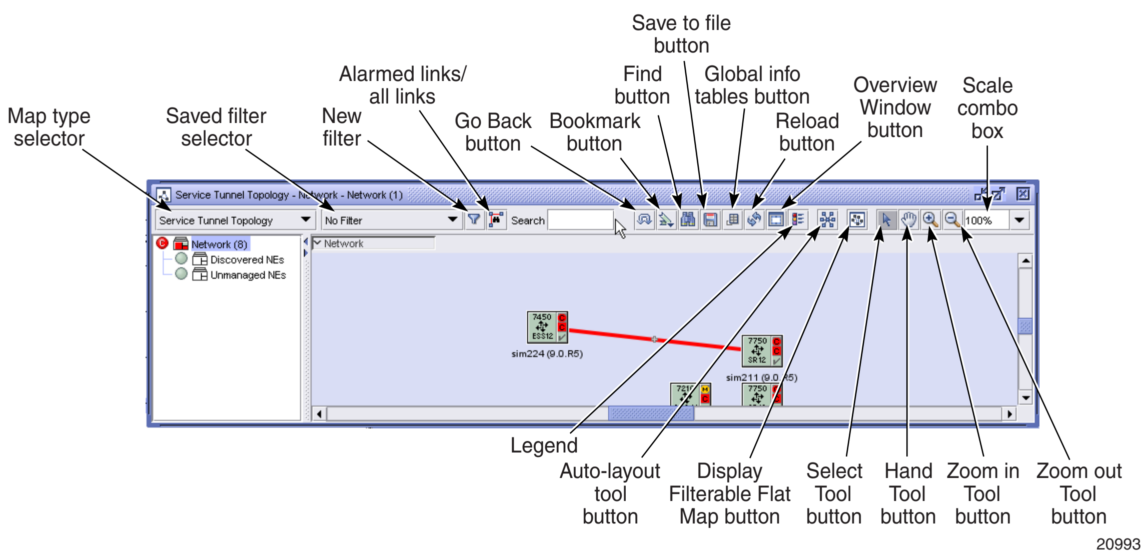


Table 5-1 describes the map toolbar elements.

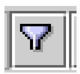
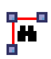
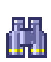
Caution 1 — Applying an information table configuration to many objects on the map may take a long time.

Caution 2 — When you reload a map from the database, the database is unavailable during the loading period.

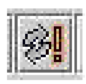
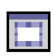
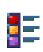
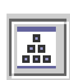
Caution 3 — The current composite service map is redrawn when you click on the Rearrange by Service Tiers button, and the prior layout of the composite service map cannot be recalled.

Caution 4 — After you click on the Auto-Layout Tool button and confirm the action, any existing map layout is overwritten and cannot be recovered. If you are satisfied with the layout of the icons on the map, do not use the Auto-Layout Tool button.

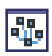
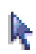
Table 5-1 Map toolbar elements descriptions

Toolbar element name	Description
Map type selector	The map type selector is a drop-down menu that lists the map view options that you can choose to specify the view. The map type selector offers the following views: • Physical Topology • Service Tunnel Topology
New Filter button 	A filter allows you to apply one or more object filters to a map view, to narrow the range of objects that are displayed. Filters can be saved for future searches on similar objects. When a filter is applied, the name of the filter is displayed on the saved filter selector. When a filter is applied, only the objects that the filter returns are displayed, with the following exceptions: • if one link endpoint is displayed, the other endpoint is also displayed, even if the filter excludes it • if a filter does not include a link filter, only the links between the returned NEs are displayed. Filters can be saved as private or public. You can apply a span of control to public filters to filter out objects that are not in the current user span of control. Public filters can only be changed by the user who created them. Private filters appear only for the user who creates them. Click on the Filter button to create and save filters that specify the objects displayed in a map. You can create a filter based on a combination of search criteria. Figure 5-4 shows the navigation buttons that you can use to create, apply, and save a map filter. See Procedure 5-21 for more information about creating a topology map filter. See chapter 3 for more information about configuring filters.
Alarmed links/All links shown button 	Click on the Alarmed links/All links shown button to specify any of the following on the topology map: • all links • only link groups with associated alarms • only specific links with associated alarms • link groups and the specific links within the link groups with associated alarms The Alarmed links/All links shown button options are: • All links shown (default)—the icon is displayed in white and all links are displayed on the map. • Show Only Alarmed—the icon is displayed in yellow and only link groups with associated alarms are displayed on the map. • Enable Alarm Link Pullout—the icon is displayed in yellow and links with associated alarms are displayed on the map. The link groups containing the pulled out alarm links with unknown physical characteristics are displayed in grey.
Go Back button 	Click on the Go Back button to navigate between previously viewed topology groups. For example, if you are viewing Router Group 1 then view Router Group 2, click on the Go Back button to return to Router Group 1. The Go Back button only functions in one map type; both previously viewed topology groups must be the same map type.
Bookmark button 	Bookmarks are used to create shortcuts to frequently visited locations on a map. Click on the Bookmark button and choose to add a bookmark or manage existing bookmarks.
Find button 	Click on the Find button to search for network objects on a map. You can choose to search for specific vertices or edges. A list form opens that allows you to configure specific criteria to filter the results of your search. See chapter 3 for information about performing searches. When the network object is found, the map navigation tree displays the topology group that contains the object. If necessary, the 5620 SAM scrolls to the part of the map where the object is located.

(1 of 3)

Toolbar element name	Description
Save To File button 	Click on the Save To File button to save the map view or the full map. You can choose the location to save the map image and the file type. See Procedure 5-8 for more information about using the Save To File button.
Global Info Tables button 	Click on the Global Info Tables button to create information table configurations, apply information table configurations globally, or turn the global information table option off. See Procedures 5-15 and 5-16 for more information about using the Global Info Tables button. See Caution 1 above.
Reload Button indicating no database changes  Reload Button indicating database changes 	Click on the Reload button to load the topology map from the 5620 SAM database. The topology map is updated to display the latest configurations. The Reload button icon changes to indicate whether moving a map object and changing the layout of the object is saved to the database. See Caution 2 above.
Overview Window button 	Click on the Overview Window button to open the Overview window. Use the Overview window to pan the entire map, or a specific group or service, and the area that you want to view. Figure 5-3 shows the Overview window.
Legend button 	Clicking on the Legend button opens a contextual menu that displays a list of map legend types, if multiple legends are available, or opens the Legend form. Choosing a legend type from the contextual menu opens the Legend form with the appropriate legend tab displayed. The following legend types are available, depending on the map type: • icons—always shown; displays the icons used to identify objects • colors—displays the color scheme used for identifying map objects • highlight sessions—displays the highlight sessions for the current map, and allows clearing of one or more sessions • other legend types that are specific to a type of map
Rearrange by Service Tiers button 	The Rearrange by Service Tiers button is available only for composite service topology maps. Figure 5-13 shows the composite service map. Click on the Rearrange by Service Tiers button to organize the composite service tier icons in the map panel by service tier. The service tier icons are displayed in the following order from the top of the panel: • tier 1 icons (typically IES and VPRN services) • tier 2 icons (typically VPLS and MVPLS) • tier 3 icons (typically satellite HVPLS and VLL services) • tier 4 icons (typically VLAN services) . . . • tier n icons (user-assigned) See Caution 3 above.

(2 of 3)

Toolbar element name	Description
Auto-Layout button[1] 	Click on the Auto-layout button to lay out the map icons. The layout options are: • Circular — emphasizes ring and star topologies in networks. Objects are grouped according to the network structure and arranged in circles or radial tree structures. • Smart Organic—emphasizes inherent data groupings and symmetries. This information helps with understanding the interconnections of complex structures. • Endpoint Layout (VPLS, VLL, mirror, and composite service sites only) - all endpoints are snapped close to the associated parent site. The Auto-Layout tool is useful when: • many newly discovered NEs are tiled together on the map and difficult to view • a large number of network device icons are spread out across the map and cannot be easily viewed without zooming out After you click on the Auto-Layout button, icons with links between them are placed closer together in the center of the map. Icons without links are placed on the periphery of the linked icons. See Caution 4 above.
Display Filterable Flat Map button 	Click on the Display Filterable Flat Map button to quickly display a flat map of the current topology map view. You can also view a flat map on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu.
Select Tool button 	Click on the Select Tool button to select and move an object on the map or to view object information. You can select and move multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all the objects you want to select on the topology map.
Hand Tool button[2] 	Click on the Hand Tool button to switch to a pan mode. Click on the background to move the contents of the map in any direction. When you are in the pan mode and you scroll over an object, you can select and move an object on the map or view object information. You can select and move multiple objects by pressing the Shift key and clicking on the object you need to select.
Zooming in  and zooming out  using a mouse or toolbar buttons[3]	The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. Click on the Zoom in Tool and Zoom out Tool buttons and click on the map to resize the objects in a map or use the mouse wheel to zoom in and zoom out of topology maps. Click on the map and roll the mouse wheel forward to zoom in or roll the mouse wheel backward to zoom out. Each roll of the mouse wheel brings the map objects closer or further. When a map is at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed at a high zoom level, the icons are displayed at normal size, link lines are thicker and labels are displayed.
Scale combo box	Use the scale combo box to increase or decrease the map zoom. You can choose a zoom percentage value from 25% to 300%, or fit all objects in the window from the drop-down menu. The scale combo box displays the current scale of the map.

(3 of 3)

Notes

(1) You can also apply the auto-layout option to a contiguous group by right-clicking on one of the selected objects. See Procedure 5-23 for information about using the auto-layout function.

(2) You can temporarily activate the panning function by pressing and holding the space bar, and then clicking in the map panel.

(3) Object icons are displayed at a reduced size in a flat map.

Figure 5-3 shows the Overview window.

Figure 5-3 Overview window

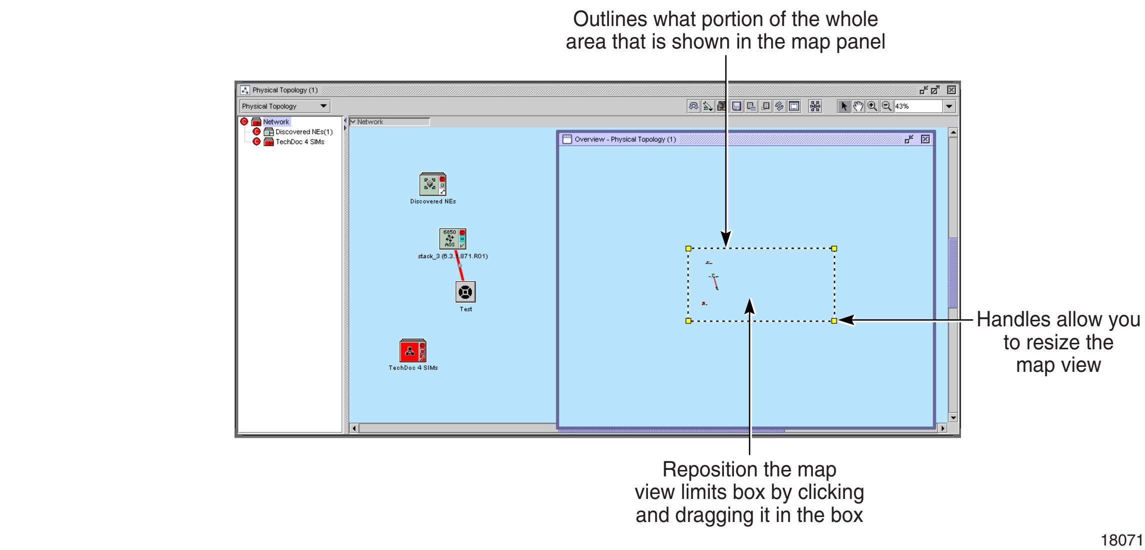
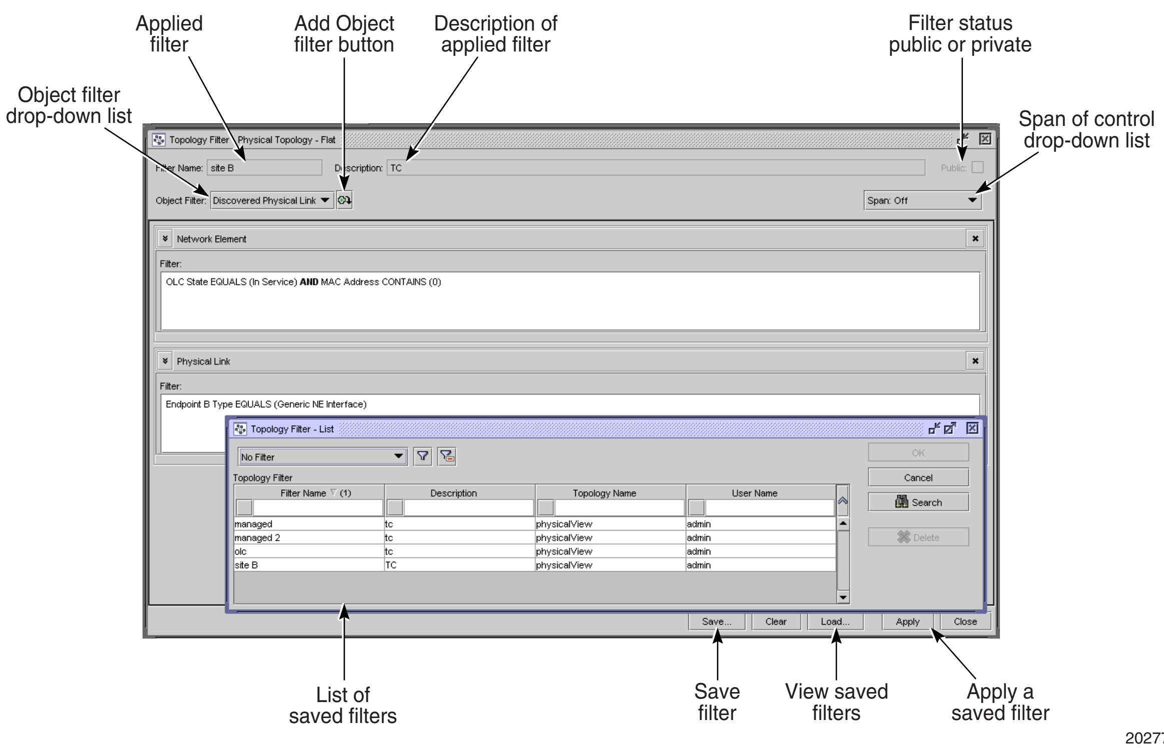


Figure 5-4 shows the navigation buttons that you can use to create, apply, and save a map filter.

Figure 5-4 Filtered map form



Zooming in and out

The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. See Procedure 5-11 for information about zooming functions.

When a map is viewed at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed a a high zoom level, icons are displayed at normal size, link lines are thicker and labels are displayed.

Bookmarks

You can bookmark frequently visited areas of the map for easier navigation when you return to those locations. Bookmarks are associated with a map view. To use the bookmark, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map. Otherwise, the bookmark menu option is disabled.

You can access the bookmark drop-down menu using the Bookmark button on the map toolbar. Figure 5-2 shows the Bookmark button. The bookmark menu is divided into two sections and separated by a horizontal line. The top section of the drop-down menu contains the bookmark management functions, and the bottom section contains the user-created dynamic list of bookmarks.

The list of bookmarks is updated when you add, remove, group, or rearrange the bookmarks. The menu items can be bookmarks or folders, which can expand to display more bookmarks or folders.

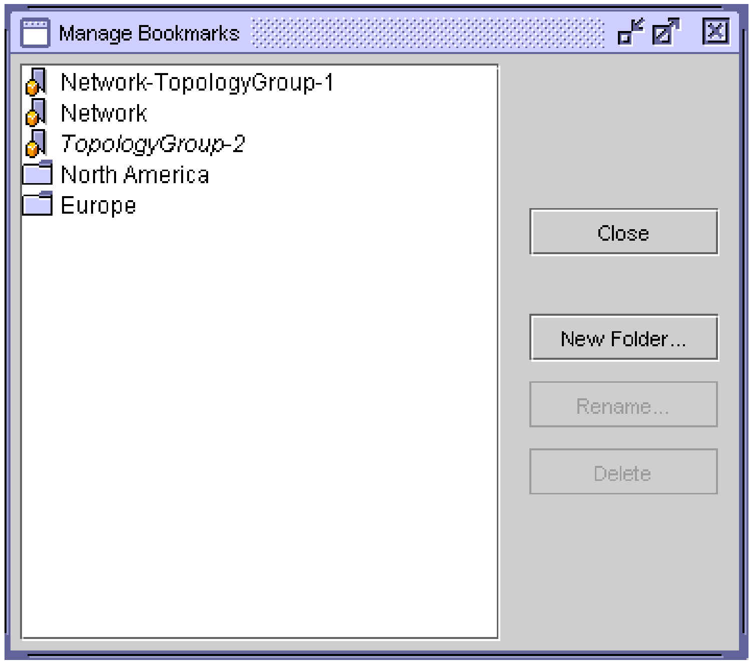
Note — A large number of bookmarks is difficult to manage. Bookmarks should be organized in folders for better usability and easier management. Alcatel-Lucent recommends that you create a maximum of 1000 bookmarks.

When a bookmark is selected, the map panel displays the bookmarked topology group. The map navigation tree expands to display the topology group.

When a valid bookmarked topology group is moved to another group, the bookmark for the group is updated to correspond to the new location of the group. If the bookmark location is not valid, for example, a topology group was deleted since the bookmark was created, an invalid bookmark message is displayed. The map panel remains unchanged.

Click on the Add Bookmark menu option to add the topology group currently viewed in the map panel as a bookmark. Click on the Manage Bookmarks menu option to open the Manage Bookmarks form. Figure 5-5 shows the Manage Bookmarks form.

Figure 5-5 Manage Bookmarks form



The Manage Bookmarks form has a list panel on the left in which the bookmarks and folders are listed in a tree structure. You can drag and drop bookmarks and folders in and out of other folders in the list panel. Select a bookmark or folder for editing. Click on an empty area to deselect the tree object. Double-click on a top-level folder to open the folder and display its contents. A turner to the left of the descendant folder object in the list panel indicates that the folder contains descendant objects, such as bookmarks or other folders.

The names of invalid bookmarks, and bookmarks and folders that are not from the current view, are displayed in italics.

The following buttons with which you can perform different actions are displayed to the right of the list panel:

- Close—used to close the Manage Bookmarks form. All changes in the form are saved when you click on the Close button.
- New Folder—used to create a folder in the list panel. The Folder Properties dialog box appears.
    - If a folder is selected in the list panel, the new folder that is an immediate descendant object of the selected folder.
    - If no folder is selected in the list panel, the new folder is created as a top-level folder.
- Rename—used to rename a folder or bookmark. The Rename dialog box appears. The Name field contains the name of the selected folder or bookmark. This button is enabled only when a folder or bookmark is selected in the list panel.
- Delete—used to delete a selected folder or bookmark from the list panel. This button is enabled only when a folder or bookmark is selected.

Information tables

You can configure information tables that are displayed beside map objects. An information table contains specific values, such as an NE chassis type, software descriptor, and system address. Information tables are displayed beside each map object to which the configuration applies. You can drag and drop information tables on topology maps, but the new table location is not saved with the map.

Note — You cannot apply an information table configuration to link groups or topology groups.

Multiple information tables can be applied to map objects, but only one is displayed at a time. Tab indicators appear on the information table to indicate that multiple information tables apply to the map object. You can cycle through the applied information tables by clicking on the information table and pressing the Tab key.

You can specify that information tables are to be displayed only during a mouse-over operation, which is when the mouse pointer passes over an object. You can also specify whether an information table contains a header. Header display is enabled by default, and cannot be disabled for mouse-over tables. See Procedure 5-15 for more information. Mouse-over supports cycling between tables using the Tab key.

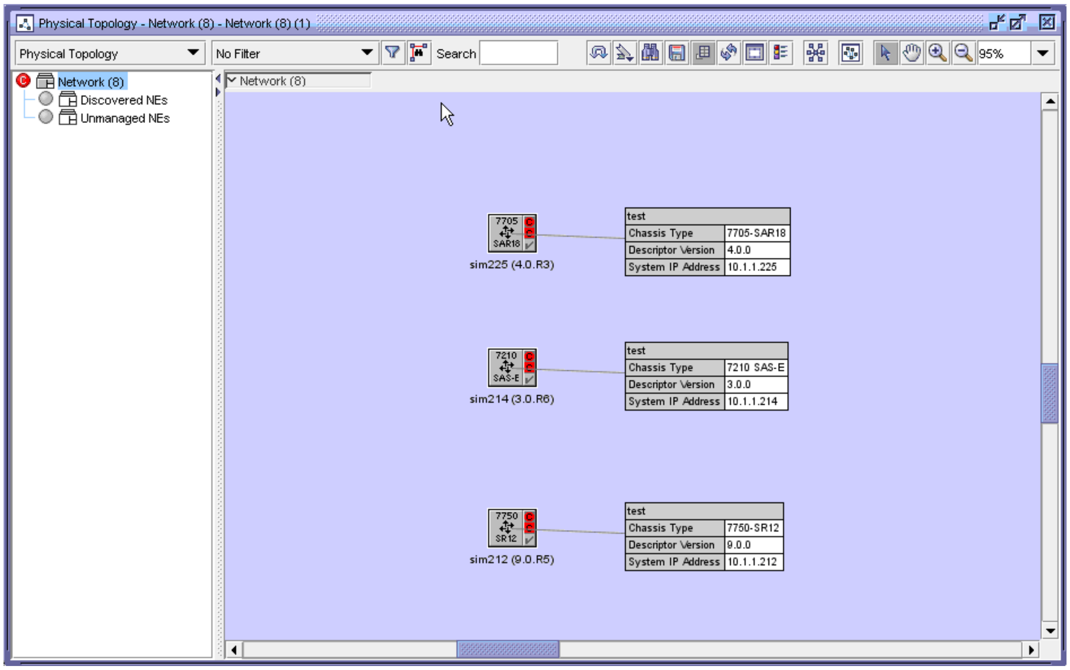
The following types of information tables can be applied to map objects:

- global—available for all map types
- selected—available for all map types
- highlight—available for maps that support the highlight function
- others that are specific to a map type

Global Info Tables

When one or more information table configurations are available for a map type, you can apply an information table configuration to all map objects using the Global Info Tables button. You can also use this button to turn the global information table configuration off. See Procedure 5-16 for more information about how to use the Global Info Tables feature. Figure 5-6 shows a map view with an information table configuration applied to all map objects.

Figure 5-6 Applied global information table configuration



Selected Info Tables

You can apply an information table configuration to one map object or a selected group of map objects by right-clicking on the object or selected group. You can also use this contextual menu to turn the selected information table configuration off. See Procedure 5-17 for information about how to use the Selected Info Tables feature.

Map Highlight Info Tables

On a map that supports the highlight function, you can apply an information table configuration to a map highlight by right-clicking on an existing highlight session from the Highlight Sessions tab of the Legend-*topology* form. You can also use this contextual menu to turn the highlight information table configuration off. See Procedure 5-18 for more information about how to use the Map Highlight Info Tables feature.

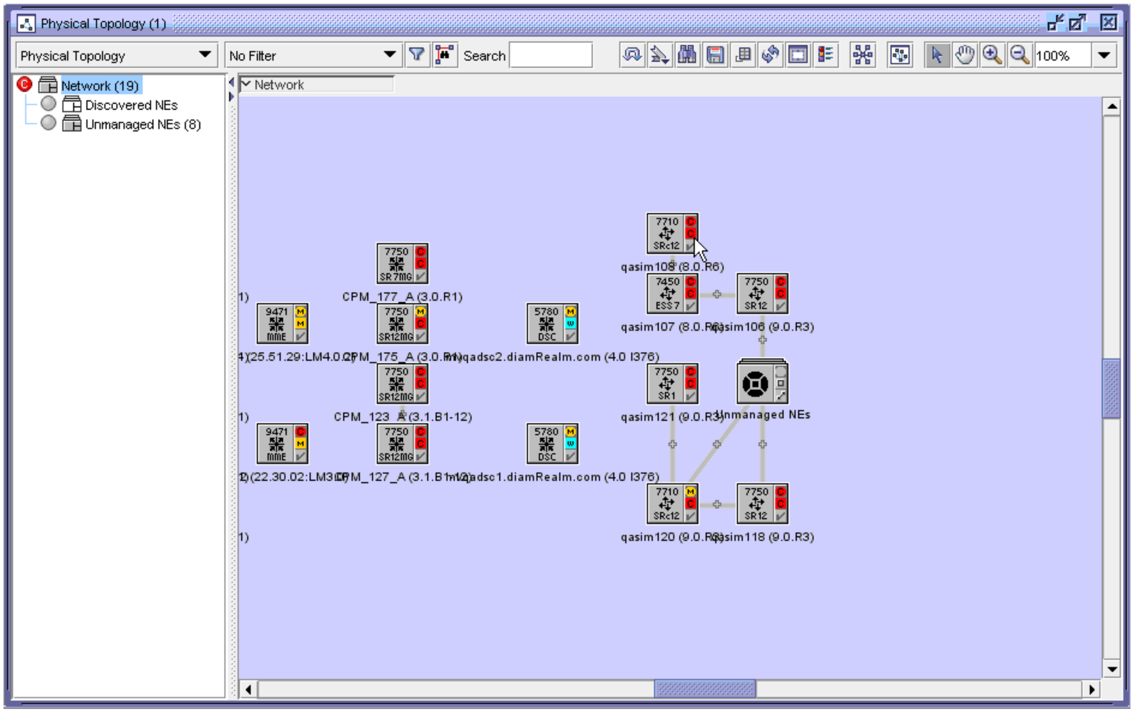
5.2 5620 SAM map types

This section details the types of maps available to the 5620 SAM.

Physical topology map

The physical topology map is available by choosing Application→Physical Topology from the 5620 SAM main menu. The physical topology map is used to view and manage Layer 1 objects, including the logical grouping of devices. Figure 5-7 shows the physical topology map.

Figure 5-7 Physical topology map



The physical topology map is open in the working panel by default when the 5620 SAM client GUI starts.

The following apply to link objects in the physical topology map:

- The following colors indicate link status:
  - Red—the link has failed
  - Light Gray—the link is in service
  - Green—the link is new
  - Blue—the link is in standby or backup mode
  - Dark gray—the link is unknown
  - Purple—the link is being diagnosed
  - Magenta—the link carries hidden links
  - Yellow—the LAG link is degraded (one or more links in the LAG have failed)
- If endpoint B of a physical link is on an unmanaged device, the status of the physical link is the same as the status of endpoint A, which is on a 5620 SAM-managed device.
- A LAG link is represented as a single physical link. However, if you right-click on a LAG link, the form that opens provides information and configuration options for the entire LAG link. For example, the Endpoint Info tab on the Discovered Physical Link form shows the link endpoints as LAG endpoints rather than physical ports, and allows the operator to open the LAG properties form.

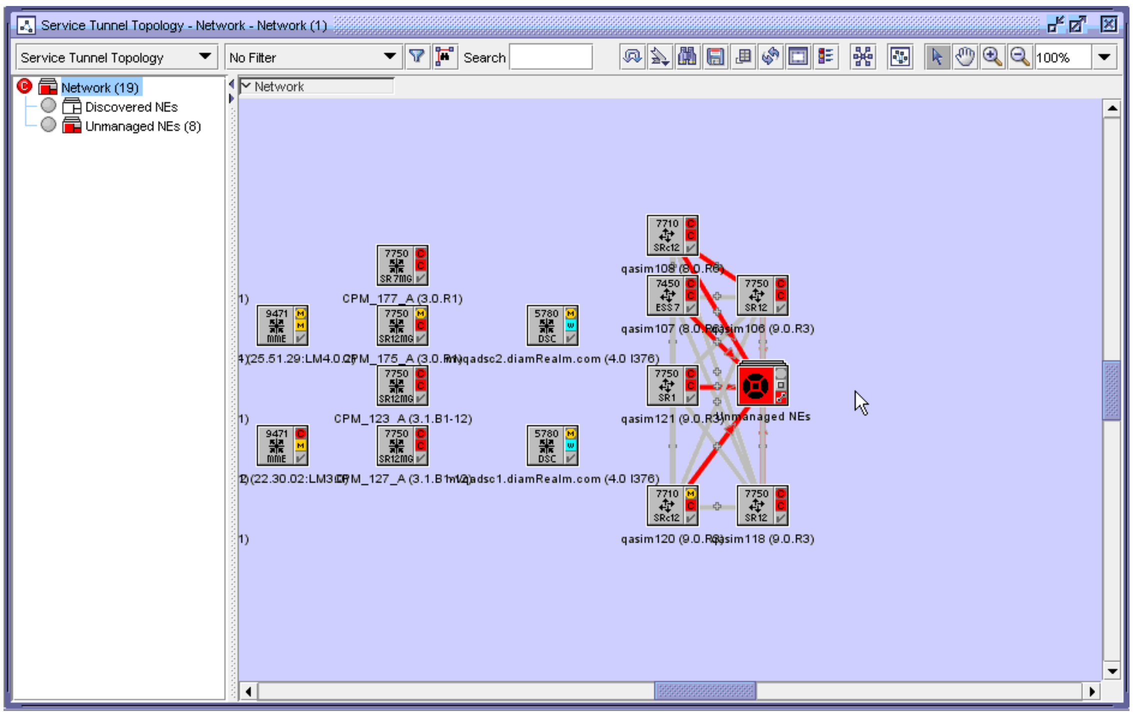
Menu options for physical topology map background

To open a contextual menu for the map background, right-click on the map background. See Table 4-2 for contextual menu option information.

Service tunnel topology map

A service tunnel topology map is available on the 5620 SAM by choosing Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map is displayed, as shown in Figure 5-8.

Figure 5-8 Service tunnel topology map



Icons in the service path topology map represent devices. The color of the device icon represents the status of the device. Red indicates that the device is down. Green indicates that the device is up. Yellow indicates that the device is being synchronized.

Link groups between devices represent service tunnels. When a link group is red, at least one tunnel in the link group is down. For link groups between managed devices, right click on the link group icon to list and edit tunnels in the link group. For link groups between managed and unmanaged devices, right-click on the link group icon to open contextual menus and submenus which allow you to open additional information forms for the service tunnel, including the properties form.

EPS path topology maps

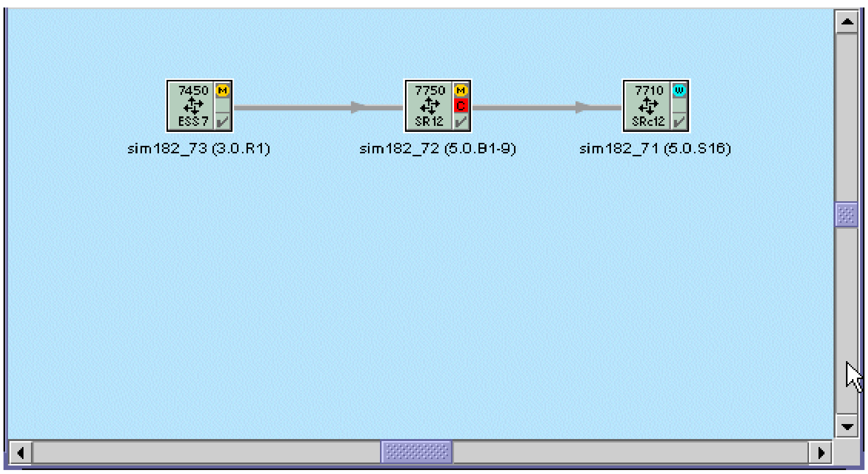
An EPS path topology map is available on the 5620 SAM by choosing Application→EPS Path Topology from the 5620 SAM main menu. See the *5620 SAM LTE ePC User Guide* and the *5620 SAM LTE RAN User Guide* for information about EPS paths in LTE networks.

LSP path topology map

An LSP path topology map is available from the MPLS Path form and the LSP Path form. See Procedure 5-3 to view the map from the MPLS Path form. See Procedure 5-4 to view the map from the LSP Path form.

The LSP path topology map is used to view a specific provisioned, actual, or CSPF LSP path in the context of its source, and transient and destination hops. Figure 5-9 shows an LSP path topology map.

Figure 5-9 LSP path topology map



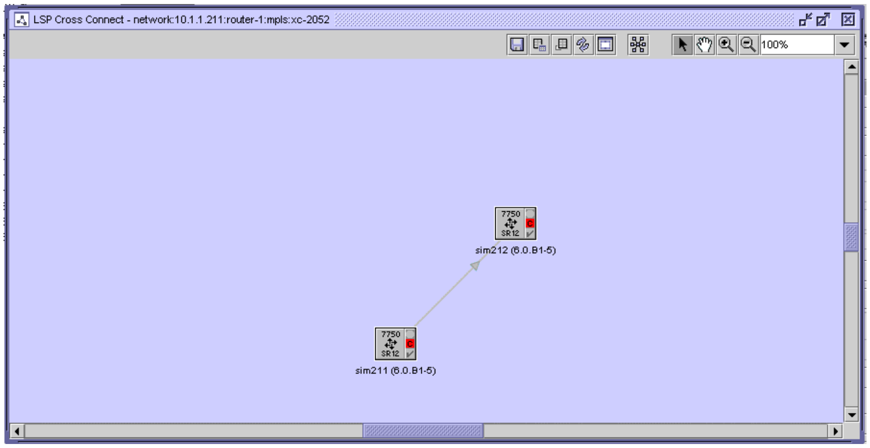
When you view the LSP path topology map, hops are linked by straight lines, where each line represents a sub-path between two hops of the LSP path. The direction of each path is indicated by an arrow. Green lines indicate provisioned paths, and gray lines indicate actual paths.

LSP cross-connect topology map

An LSP cross-connect topology map is available from the LSP Path form. To view the map from the LSP Path form, see Procedure 5-6.

The LSP cross-connect topology map is used to view a specific LSP cross-connect in the context of its source, and transient and destination hops. Figure 5-10 shows the LSP cross-connect topology map.

Figure 5-10 LSP cross-connect map



Flat maps

Flat maps provide a complete network view without topology groups. A flat topology map can display up to 1000 objects. You can narrow the range of objects that are displayed by creating and saving filters and filter definition trees.

A flat map is available on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu. The following flat map types are available:

- Physical Topology
- Service Tunnel Topology

A flat map is used to view a large number of network objects and link groups. You can double-click on a NE in the flat map to display the object properties. For example, when you double-click on an NE, a property form opens, from which you can view or configure the NE parameters.

Object icons in a flat map are displayed at a reduced size, link lines are thinner, and object information is not displayed. Flat maps support the following, as do other 5620 SAM topology maps:

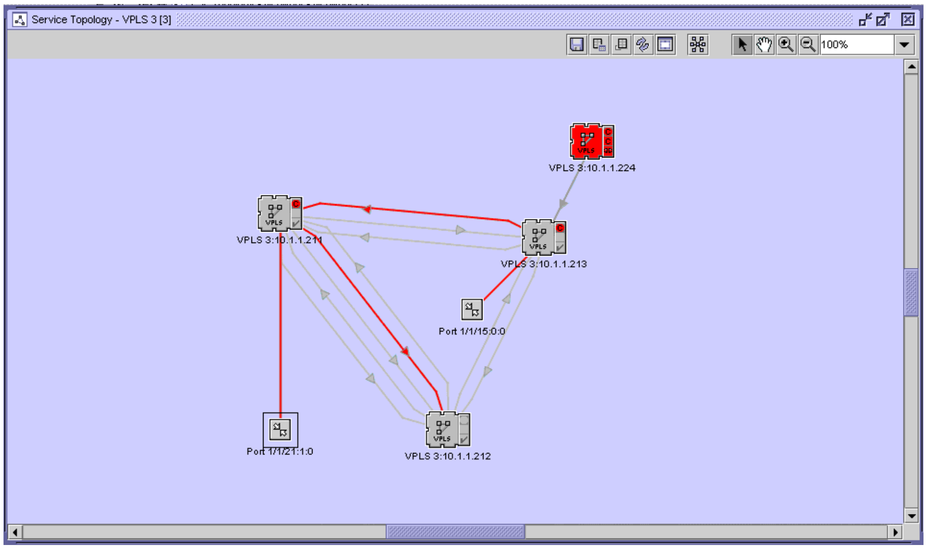
- mouse-based navigation
- zooming
- NE and link status colors
- searching
- filtering

Service topology maps

A service topology map is available from the Manage Services form. To view the map from the Manage Services form, choose Manage→Service→Services from the 5620 SAM main menu and list services by clicking on the Search button. Select one or more services in the list and click on the Topology View button.

Figure 5-11 shows the service topology map.

Figure 5-11 Service topology map



The large icons represent managed devices. The small icons represent unmanaged devices. The label of the managed device icon indicates the service name and the IP address of the device.

The symbol and color in the top-right corner of the managed device icon represents the aggregated alarm status, the most severe alarm on any of the services on the device. The symbol immediately below the aggregated alarm status symbol on the icon and the color of the icon together indicate the alarm status for the service site. A red icon indicates that the service on the device is down. A green icon indicates that the service on the device is up.

The port icons represent managed access interfaces. A service site can support up to 20 SAPs. When the number of SAPs on a service site exceeds 20, all of the SAPs on that site are grouped into a SAP group, represented by a SAP group icon on the map. When the number of SAPs drops below 20, the SAP group icon is replaced with the icons for all the individual SAPs on the map. To view the list of SAPs in a SAP group, right-click on the SAP group icon and choose List L2 Access Interface or List L3 Access Interface, depending on the service type, from the contextual menu. The corresponding Site form for the service opens with the L2 Access Interface or L3 Access Interface tab is displayed.

A line between two map objects represents a link or group of links. Links between device icons represent service circuits. Links between device icons and port icons represent the binding of an access port or interface to a service. The symbol and color in the bottom right corner of the managed device icon represents the connectivity alarm status. During a resynchronization of the managed device, the icon represents the resynchronization status, and is shown in yellow. The status is inherited from the link endpoints. A plus sign icon located in the centre of the link indicates a bidirectional group link. An arrow icon located on the link indicates a unidirectional link and identifies the direction of the path.

Right-clicking on a managed NE, port, or link opens a contextual menu. Contextual menus allow you to open additional information forms, such as the properties form for an object.

You can view multiple services on a map at the same time if the services are selected from the Manage Services form during map creation.

Service segmentation

A service segmentation view is also available to aid in conceptualizing complex services. Segments are logical grouping of interconnected sites, services, and bindings. The segmentation view is available for VPLS and VLL services.

A service segment is considered to be a portion of a single service that extends to multiple sites connected within that segment. It is based on the service type through one of the possible connection topologies (for example, mesh, PBB tunnels, a switching VLL, rings, and so on), without having to pass through any connectors such as spokes, CCAGs, or SCPs (SAP-to-SAP).

General examples of segments in Layer 2 service topologies include:

- A simple pair or single spoke/mesh SDP binding comprises one segment
- A mesh of a multi-node VPLS service comprises one segment
- A multi-node mesh with a spoke SDP to a single node comprises two segments
- Each mesh of VSIs forms a segment (applicable to H-VPLS)

Just a few examples of the many possible service-specific segmentation configurations include scenarios such as the following:

- H-VPLS (Inter-Metro with redundant spoke SDPs):
    - One application of H-VPLS is the connection of two or more geographically-dispersed VPLS domains belonging to the same customer. Two spoke SDP connections are used to connect each VPLS between the two metros, either in a redundant PW spokes topology or under STP protocol. The redundant spokes comprise one segment, while each VPLS will also comprise one or more segments, depending on their specific configurations.
- VLL Switching:
    - For a VLL service at a switching router, a terminating PE device has at least one VLL SAP, while a switching PE device has a VLL instance which cross-connects two spoke bindings. All VLL instances of such a service must have the same service ID, and if the VLL has one or more switching sites, it must have at least two terminating sites. In this scenario, the primary and redundant spoke SDPs on the same network endpoint are considered to be in the same segment.
- PBB:
    - In a PBB configuration, the B-VPLS is considered a service tunnel, from the I-VPLS or I-Epipe perspective. Therefore, the sites connected via a B-VPLS (that is, having the same ISID) are considered to be in one segment.
    - I-Sites bound to the same PBB tunnel (B-VPLS) and having the same ISID exist in the same segment.
    - Epipe sites bound to same PBB tunnel (B-VPLS) exist in the same segment

Whenever you modify a service, note that the following actions can trigger segment creation, modification, or deletion in a segmented service view:

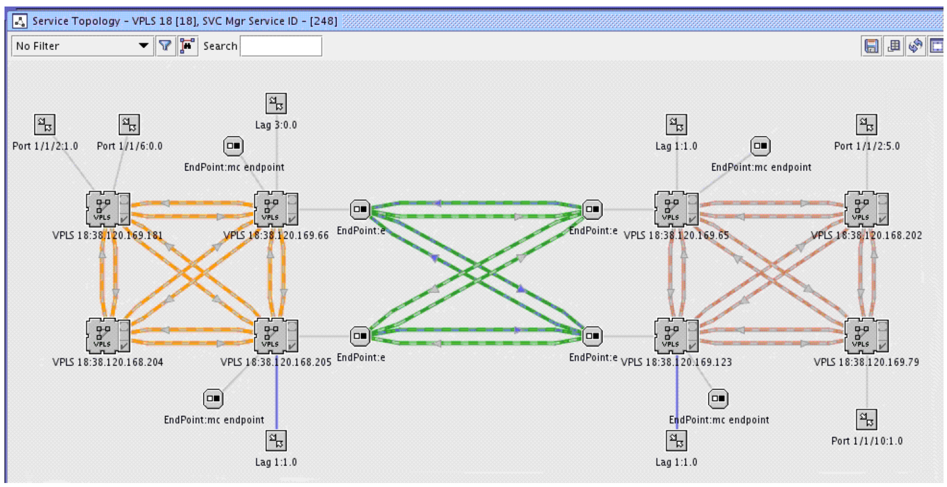
- Adding or removing service sites
- Creating or deleting spoke and/or mesh bindings (either through the 5620 SAM GUI or CLI)
- Creation or deletion of VLAN Uplinks by 5620 SAM

You can access the segmented view of a service by right-clicking on an empty portion of the background in the service's topology view. A contextual menu allows you to activate or de-activate the segmented view for the service.

In a segmented view, the outlined links of all spoke bindings, mesh bindings, or VLAN Uplinks are colored in the same distinct way for the segment they belong to. However, there are currently only 19 different colors available for use in showing service segments. If all the colors for a specific service are used, a warning message is logged to indicate this.

Figure 5-12 shows an example of how the 5620 SAM displays the segmented view of an H-VPLS Metro-to-Metro service.

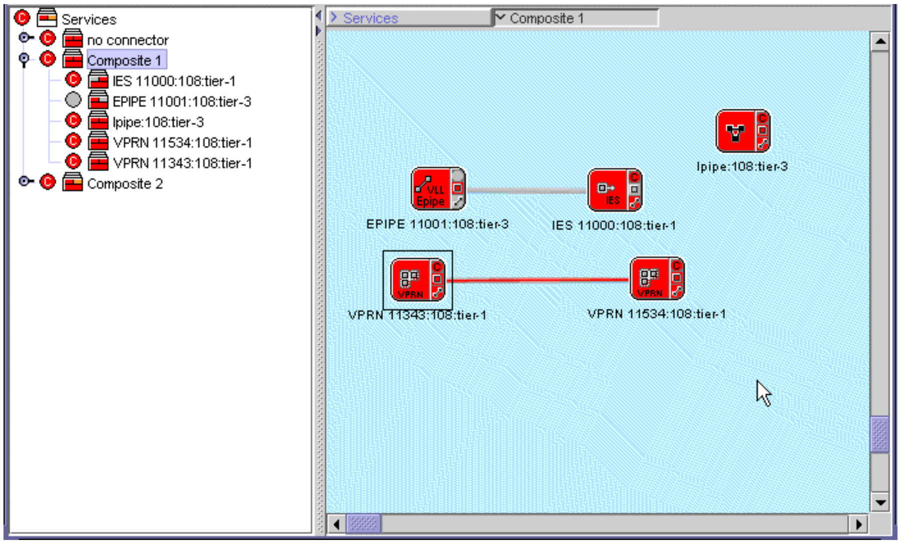
Figure 5-12 Service segmentation example



Composite service topology maps

You can use the 5620 SAM to view composite service topology and flat topology maps. Figure 5-13 shows a sample composite service topology map. When you open a flat topology view map, the navigation tree is not part of the map.

Figure 5-13 Composite service topology map



In a composite service topology map, you can use the navigation tree at the left side to display the composite service and service tier hierarchy starting from the services object. The map navigation tree displays the following:

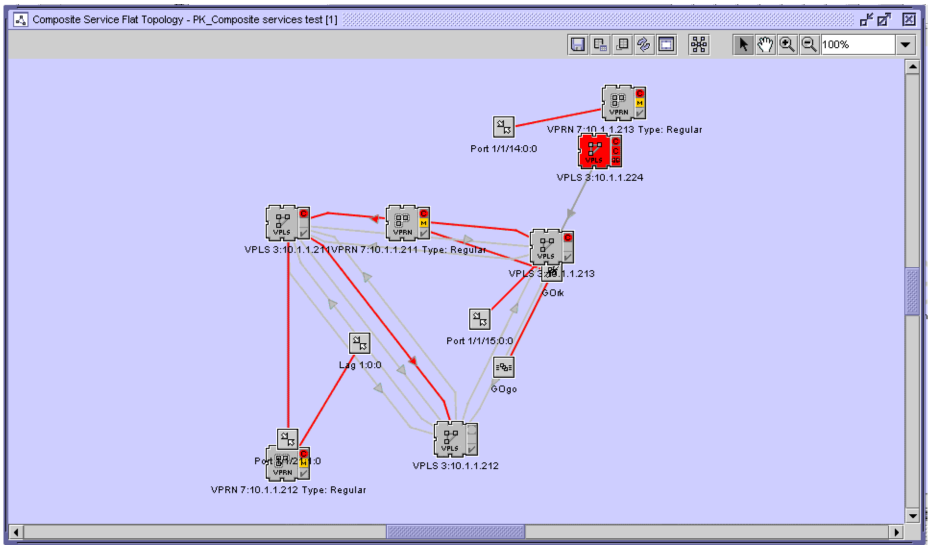
- composite services and service tiers, including service name and tier number
- status of the composite services and their tiers

The map toolbar for the composite service topology map includes the Rearrange by Service Tiers button. See Table 5-1 in this section for more information.

Double-click on a composite service object in the map panel to display the service objects that belong to the composite service. Double-click on the service objects to display the service sites and access interfaces. The links or groups of links between the service sites and access interfaces are also displayed.

In the composite service topology map, all service objects in the composite service are displayed simultaneously. The service sites, access interfaces, and the links or groups of links between them are also displayed. The navigation tree is thus not required in this view. Figure 5-14 shows a sample composite service flat topology map.

Figure 5-14 Composite service flat topology map



You can right-click on an object icon or link group icon to turn up, shut down, or display the properties form for the item.

5.3 Working with maps

This section details different methods of managing 5620 SAM capabilities from the topology view.

Modifying a service from the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view in the service configuration forms.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

Services that can be modified from their topology views include VPLS, VPRN, VLL, IES, and composite services. See the appropriate service management chapter for procedures that describe how to modify services from the topology view.

Managing OAM diagnostics from the topology view

A 5620 SAM operator can configure and execute OAM diagnostic tests from the service topology view. A right-click contextual menu of test types and test operations allows a GUI user to perform many test-management tasks. The OAM diagnostic functions on the map are enabled and disabled using a selector in the map window.

5620 SAM OAM diagnostic test management using the topology map is supported for the following service types:

- VLAN, excluding 9500 MPR VLAN
- VLL Epipe
- VPLS
- VPRN

You can use a contextual menu option to open a test-creation form for selected map objects such as NEs, SAPs, SDPs, MEPs, and MIPs. The form is automatically populated with the information for the selected objects. After you apply the test configuration, you can use the map to execute the test and view the results. A test result summary is viewable using statically displayed or mouse-over global info tables that are shown beside the object that initiates the test. By default, the info table for a tested object displays the five most recent test results; you can enable or disable the display of individual or all results.

The general OAM contextual menu options that are available include the following:

- Create OAM Tests—lists the tests that are appropriate for the service type and selected objects; choosing a test type opens the pre-populated test-creation form
- Select OAM Tests—opens a filterable list form from which you can choose previously created tests associated with one or two objects

Note — The tests that are listed using the Select OAM Tests option do not include generated tests, or manually added first-run or last-run tests in a test suite.

See Procedure 5-28 for information about enabling basic OAM-related map functions.

Working with Ethernet CFM objects

You can configure and manage Ethernet CFM objects such as MEGs, MEPs, and MIPs using the Ethernet CFM contextual menu option. MEPs and MIPs are represented iconically. For example, a SAP or SDP binding object can have a graphical connector to MEPs and MIPs, and a site object can be connected to a B-VPLS MEP.

A service topology map displays only one MEG at a time. The MEG is selectable using a drop-down list in the map window when the OAM function on the map is enabled. The CFM objects associated with the currently selected MEG are displayed.

For a MEP, the following attributes are displayed:

- the MEP level, as a number inside the icon
- the MEP direction, as the up or down direction in which the icon points
- the MEP administrative state, as the icon color

For a MIP, only the level is displayed.

The displayed Ethernet CFM contextual menu options for MEPs and MIPs depend on the Ethernet CFM configuration, for example, the MD level and whether MEPs and MIPs are already present in the MEG.

When an operator right-clicks on the map background, the available Ethernet CFM option is global MEG creation, which opens a configuration form populated with the selected sites or all service sites, if none are selected.

When the selected object is a SAP, you can create, view, and delete MEPs, however MEP creation in this context is limited to B-VPLS sites. You can enable, disable, and view MIPs. Enabling a MIP creates a MIP only when the configuration supports this function.

When the selected object is an SDP binding, you can enable, disable, and view the associated MEPs.

Note — When you enable a MIP on a SAP or SDP binding, the 5620 SAM creates a MEG site if one does not exist, and uses explicit MHF creation.

5.4 Workflow to use 5620 SAM maps

1. Familiarize yourself with the components and basic operations of 5620 SAM maps. See sections 5.1 and 5.5 for more information.

2. Determine the map type you want to use. See section 5.2 for more information.

   - Select service maps to show which NEs are used by the services.
   - Select topology maps to show the relationship between NEs in a routing domain.

3. Configure map layout and object information tables. See section 5.6 for more information.

4. As required, create map filters to narrow the range of objects displayed. See section 5.6 for more information.

5. As required, create topology groups and populate the groups with devices to organize the network. See section 5.7 for more information.

6. As required, create physical links between managed and unmanaged devices to configure Layer 1 management. See section 5.7 for more information.

5.5 Basic 5620 SAM map procedures

Use the following procedures to perform basic map management tasks.

Procedure 5-1 To open a map from the 5620 SAM main menu

1 Choose Application from the 5620 SAM main menu.

2 Choose a type of map to view from the menu options:

- Physical Topology to view Layer 1 network connectivity
- Service Tunnel Topology to view service tunnels
- Flat Maps→Physical Topology
- Flat Maps→Service Tunnel Topology

The appropriate map opens and displays the network objects.

See Procedure 5-7 for information about using the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

Procedure 5-2 To open a service topology map

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Create an appropriate filter and click on the Search button. A list of services is displayed.

3 Select one or more services in the list and click on the Topology View button. A dialog box appears.

4 Click on the Yes button to continue. The Service Topology map opens.

See Procedure 5-7 for information about the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

Procedure 5-3 To open an MPLS provisioned path map from the MPLS Path form

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Create an appropriate filter and click on the Search button. A list of MPLS paths is displayed.

3 Select an MPLS path in the list and click on the Properties button. The MPLS Path configuration form for the MPLS path opens.

4 Click on the Provisioned Path tab button. The hops of the MPLS path appear in a list.

5 Select a hop in the list and click on the Topology View button. The MPLS provisioned path map opens showing the hops between the devices.

See Procedure 5-7 for information about the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

Procedure 5-4 To open a dynamic LSP path map from the LSP Path form

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Select a dynamic LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the LSP-Path Bindings tab button. The LSP paths appear in a list.

5 Select an LSP path in the list and click on the Properties button. The LSP-Path Binding (Edit) form opens.

6 Perform one of the following:

a View the topology for provisioned paths:

i Click on the Provisioned Path tab button. The hops of the LSP path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the hops between the devices.

b View the topology for actual paths:

i Click on the Actual Path tab button. The hops of the actual path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the actual path hops between the devices.

c View the topology for CSPF paths:

i Click on the CSPF Path tab button. The hops of the CSPF path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the CSPF path hops between the devices.

See Procedure 5-7 for information about the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

Procedure 5-5 To open a flat map

1 Perform one of the following.

  a Open a flat physical topology map.

    i Choose Application→Flat Maps→Physical Topology from the 5620 SAM main menu. The Topology Filter - Physical Topology - Flat filter form opens.

    ii Go to step 2.

  b Open a service tunnel topology map.

    i Choose Application→Flat Maps→Service Tunnel Topology from the 5620 SAM main menu. The Topology Filter - Service Tunnel Topology - Flat filter form opens.

    ii Go to step 2.

  See Procedure 5-7 for information about the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

2 Perform one of the following:

  a Perform Procedure 5-21 to create a filter definition.

  b Perform Procedure 5-22 to load and apply a saved filter.

3 View the map.

4 Close the map.

Procedure 5-6 To open a dynamic LSP cross-connect topology map

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose an LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the Cross Connects tab. The cross-connects of the LSP path appear in a list.

5 Choose a cross-connect in the list and click on the Topology View button. The LSP path map opens and displays the cross-connects between the devices.

See Procedure 5-7 for information about the map elements. See Procedure 5-9 to list or view object information from a map. See section 5.1 for information about the map views.

Procedure 5-7 To view and understand map elements

1 Open a map, as described in Procedures 5-1 to 5-6.

2 View the map elements, which can include the following:

- device icons, which each display one of the following background colors to represent connectivity status and SNMP reachability
  - red—down or unreachable
  - yellow—resynchronizing or discovering
  - green—normal

  The icon in the top-right corner of a device icon represents the most serious alarm raised against the device.

  The icon in the middle right hand side of a device icon represents the alarm status for the device.

The icon in the bottom right corner of a device icon represents the connectivity to the device. During resynchronization, the icon represents the resynchronization status; for example, yellow.

- topology group icons, which have the following characteristics:
  - The background color white indicates that the topology group does not contain any descendant objects.
  - The color and icon in the upper left corner of the topology group icon indicate the most severe alarm on any of the devices in the group.
  - The color of the upper middle section of a topology group icon indicates the aggregated connectivity status of the devices in the group.
  - The color of the upper right corner of the topology group icon indicates the aggregated link status of the links in the group.
- composite service icons, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the composite service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the composite service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the composite service.
- service tier icons in composite service maps, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the service.

Procedure 5-8 To save a map to a file

You can use the Save to File button to save a portion of a map or the entire map to a file. You can save the file in JPEG, BMP or PNG format.

1 Open a map.

2 Click on the Save To File button. The save options are displayed in the drop-down menu.

3 Choose a type of view from the drop-down menu:

- Choose Save Map View to save the current view.
- Choose Save Full Map to save the entire map view.

The Save form opens.

4 Save the results.

i To choose a directory for the file, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose BMP, JPEG, or PNG from the File of Type drop-down menu.

iv Click on the Save button. The map view is saved to the specified file.

Procedure 5-9 To view object information from a map

1 Open a map.

2 Right-click on one of the following objects:

- device icon
- plus sign icon in the centre of a link or link group
- port of a generic or unmanaged NE that indicates the endpoint of a link, path, tunnel, or service
- topology group icon

The appropriate contextual menu appears.

3 Choose a contextual menu option. The following are examples of the options available, depending on the type of object selected.

- Choose Properties to open the properties form for the object.
- Choose Scripts to open the properties form for an NE with the Scripts tab displayed.

Procedure 5-10 To manage the topology map window

The topology map panel and navigation tree panel are separated by a vertical split bar that you can use to control the panels. You can change the size, and hide, or show the map panel or the navigation tree panel.

1 To change the size of the map panel and the navigation tree panel, drag the vertical split bar to the left or right to control the amount of space used for the map panel and the navigation tree.

2 To hide the navigation tree panel, click on the vertical split bar left-facing arrow icon. The tree panel is hidden.

3 To show the map navigation tree panel, click on the vertical split bar right-facing arrow icon. The tree panel opens.

4 To hide the map panel, click on the vertical split bar right-facing arrow icon. The map panel is hidden.

5 To show the map panel, click on the vertical split bar left-facing arrow icon. The map panel opens.

Procedure 5-11 To zoom in and zoom out on a map

1 Open a map.

2 Perform one of the following:

- **a** Use the mouse wheel to zoom in and zoom out. Perform the following steps.
  - **i** Click on the map.
  - **ii** To zoom in, roll the mouse wheel forward.
  - **iii** To zoom out, roll the mouse wheel backward.
- **b** Use the Zoom In Tool and Zoom Out Tool. Perform the following steps.
  - **i** Click on the Zoom in Tool or Zoom out Tool button.
  - **ii** Move the mouse pointer into the map panel. The pointer changes to a magnifying glass containing a + or - sign.
  - **iii** Click on the area of the map you want to expand or contract. The map expands or contracts. Continue clicking until the desired zoom level is reached.
  - **iv** Use the opposite button and an equal number of clicks to return the map to its default setting.
  - **v** To return to the pointer icon, click on the Select Tool button in the toolbar.

3 Use the Scale combo box to specify a zoom level, and press ↵.

Procedure 5-12 To display only selected map objects

1 Open a map.

2 Select the objects.

3 Right-click on the selected objects and choose Show only Selected from the contextual menu. The map refreshes to display only the selected objects, and the word Hidden is displayed in the map panel to indicate that some objects are currently hidden.

4 To restore the original map view, right-click in the map panel and choose Cancel Show Only from the contextual menu.

Procedure 5-13 To display only highlighted map objects

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Show Only Highlighted from the contextual menu. The map refreshes to display only the highlighted objects, and the word Hidden is displayed in the map panel to indicate that the non-highlighted objects are currently hidden.

5 To restore the original map view, right-click in the map panel and choose Cancel Show Only from the contextual menu. The map refreshes to display the original view.

Note — You can also restore the original map view by right-clicking on the selected highlight sessions in the Legend form and choosing Cancel Show Only from the contextual menu.

5.6 5620 SAM map configuration procedures

Use the following procedures to perform map configuration tasks.

Procedure 5-14 To configure and view topology map icon labels

By default, topology map icons include a descriptive label. For example, the label on a managed device icon on the Service Topology map includes the service name and the IP address of the device.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Click on the Topology tab. A list of topology map icons is displayed.

3 Select a topology map icon.

4 Configure Text Field #1 and Text Field #2 to identify the information to display in each map icon label.

5 Click on the OK button. The User Preferences form closes.

Procedure 5-15 To create an information table configuration

You can create an information table configuration for all map objects, selected map objects, or map highlights. See Procedure 5-16 to apply a configuration to all map objects. See Procedure 5-17 to apply a configuration to selected map objects. See Procedure 5-18 to apply a configuration to highlighted map objects.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Select the Configure menu item. The *topology_view* Info Table Configurations form opens.

4 Click on the Create button. The *topology_view* - Info Table Configuration form opens.

5 Configure the Configuration Name parameter.

6 For each map object type, click on the associated check box to select the attribute for display in the information table.

Note — If an applicable attribute is not selected for a specific object type, an information table is not displayed when you apply an information table configuration to objects of that type.

7 Click on the OK button. The *topology_view* - Info Table Configuration form closes, and the new configuration is listed on the *topology_view* - Info Table Configurations form.

8 Close the *topology_view* - Info Table Configurations form.

Procedure 5-16 To enable or disable a global information table

The Global Info Tables button allows you to view an information table for all map objects. An information table configuration must be created before it can be applied. See Procedure 5-15 for information about creating an information table configuration.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Perform one of the following:

a Select a radio button to apply an existing global information table configuration. The map is refreshed with the corresponding information table displayed beside the map objects.

b Click on the Off button. The global information table feature is disabled.

Procedure 5-17 To enable or disable a selected information table

The Selected Info Tables menu option allows you to view an information table for a map object, or a group of map objects. An information table configuration must be created before it can be applied to a map object or a group of map objects. See Procedure 5-15 for information about creating an information table configuration.

1 Open a map.

2 Right-click on a map object or a selection of map objects. A drop down menu opens.

3 Choose Selected Info Tables. A drop down menu opens with a list of information table configurations and an Off option.

4 Perform one of the following:

a Choose an information table configuration. The map view is refreshed with the configured information table displayed beside the map objects.

b Choose the Off option. The selected information tables for the selected map objects are no longer displayed.

Procedure 5-18 To re-enable or disable map highlights

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Perform one of the following:

a Re-enable a disabled highlight. Perform the following steps.

i Select the check box in the Active column for the highlight.

ii Click on the Apply button. The map view is refreshed with the highlight displayed.

b Disable the highlight. Perform the following steps.

i Deselect the check box in the Active column for the highlight.

ii Click on the Apply button. The map view is refreshed. The highlight and the associated information tables are no longer displayed.

4 Click on the Close button. The Legend - *topology* form closes.

Procedure 5-19 To enable or disable a highlight information table

You must create an information table configuration before you can apply it to a map highlight. See Procedure 5-15 for information about creating information table configurations.

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Highlighted Info Sessions from the contextual menu. A drop-down menu opens with a list of information table configurations and an Off option.

5 Perform one of the following.

a Choose an info table configuration. The map view is refreshed with the chosen information table displayed beside the highlighted map objects.

b Choose the Off option. The map view is refreshed and no longer displays information tables for the highlighted map objects.

Note — When a highlight is disabled or deleted, the map no longer displays the information tables for the highlight.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 5-20 To delete a map highlight

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Click on a map highlight to select it.

4 Right-click on the selected highlight and choose Delete. A dialog box appears.

5 Click on the Yes button. The highlight is deleted.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 5-21 To create a map filter

Perform this procedure to configure a filter to restrict the objects in a map view. You can save the filter for searches on similar objects.

1 Open a map.

2 Click on the New Filter button. The Topology Filter - *topology_view* form opens.

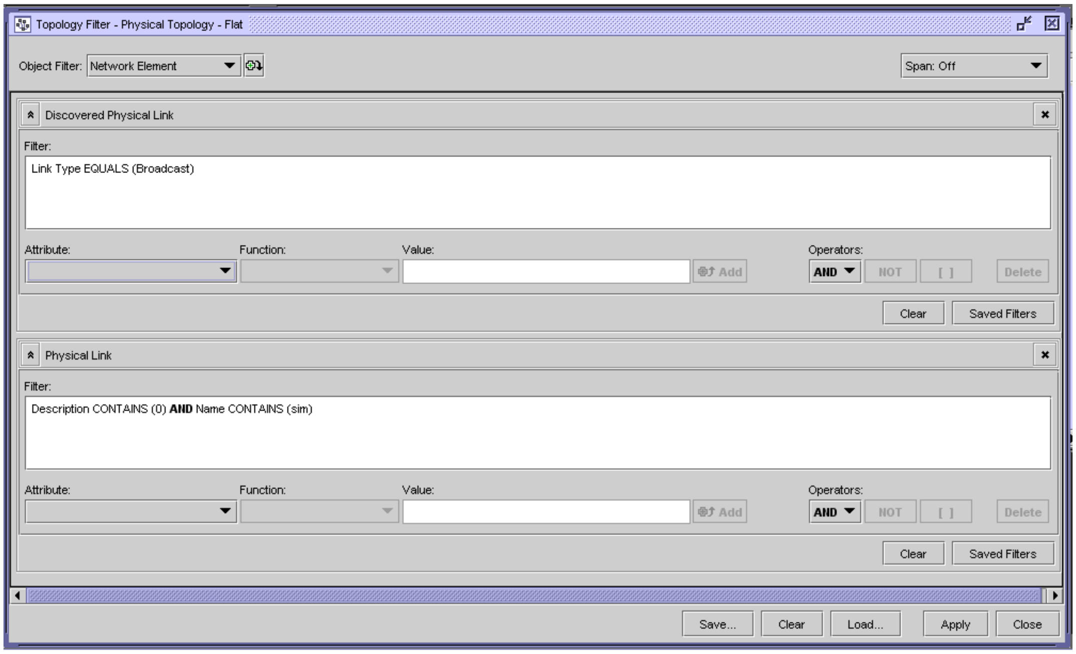
3 Choose an object filter from the Object Filter drop-down menu. Table 5-2 lists the filter options for each map type.

Table 5-2 Map filter options

Type of map	Filter options
Physical topology	Discovered Physical Link Network Element Optical Link Physical Link
Service tunnel topology	Network Element Tunnel

4 Click on the Add Object Filter button. The selected object filter is displayed in the filter panel as shown in Figure 5-15.

Figure 5-15 Map filter



5 Choose one or more of the object filters to create the filter. See chapter 3 for information about creating filters.

6 Configure the Span parameter.

7 Perform one of the following:

a Click on the Apply button to apply the filter and not save the filter. The map view is refreshed to display only the map objects defined in the filter. The filter selector displays Filter Applied.

b Perform the following steps to save the filter.

i Click on the Save button. The Save Filter form opens.

ii Configure the parameters:

- Filter Name
- Description
- Public

8 Click on the Save button. The Save Filter form closes.

9 Close the Topology Filter - *topology_view* form.

Procedure 5-22 To load and apply a saved filter to a topology map

See Procedure 5-21 for information about creating a filter definition tree.

1 Open a map.

2 Click on the saved filter selector and choose a filter from the drop-down list.

The 5620 SAM applies the filter and the map view is refreshed to display only the map objects specified in the filter. The filter name is displayed in the saved filter selector.

Procedure 5-23 To auto-layout icons on a map

Caution — After you click on the Auto-Layout button and confirm the action, the existing map layout is overwritten and cannot be recovered.

1 Open a map.

2 Perform one of the following:

a Auto-layout all of the icons on the map.

i Click on the Auto-Layout Tool button and choose one of the following options:

- Circular - emphasizes ring and star topologies in networks. Objects are grouped according to the network structure and arranged in circles or radial tree structures.
- Smart Organic - emphasizes inherent data groupings and symmetries. This information helps with understanding the interconnections of complex structures.
- Endpoint Layout (VPLS, VLL, mirror, and composite service sites only) - all endpoints are snapped close to the associated parent site.

A dialog box appears.

ii Click on the Yes button.

b Auto-layout a group of icons on the map.

i Select multiple objects.

ii Right-click on an object in the group, choose Layout Selected, and choose one of the following options from the contextual menu:

- Circular
- Smart Organic
- Endpoint Layout (VPLS, VLL, mirror, and composite service sites only)

A dialog box appears.

iii Click on the Yes button.

The map layout changes so that icons with links between them are closer together, and icons without links between them are moved to the periphery.

Procedure 5-24 To search for a specific network object

1 Open a map.

2 Perform one of the following:

a To search for a network object by typing the name, or part of the name of the network object:

i Click on the Find button in the map toolbar.

ii Choose Find Vertex or Find Link. The Find *object* form opens.

iii Configure the filter criteria and click on the Search button. A list of objects is displayed.

Note — The search function is case sensitive.

iv Select an object in the list.

b To search for a network object by pasting the name of the network object from the clipboard:

i Click on the network object that you want to locate from the equipment view of the navigation tree or from a generated or displayed list.

ii Click on the Copy to Clipboard icon to copy the network object name to the clipboard.

iii Click on the Find button.

iv Choose Find Vertex or Find Link. The Find Object form opens.

v Click on the Paste button. The network object that you copied to the clipboard is displayed in the Find object with label containing text field.

Note — Only the first item listed on the clipboard is pasted in the Find object with label containing text field of the Find Object form.

c Use the Quick-search field on the map window. Perform the following steps.

i Type part or all of the object name in the Quick-search field beside the toolbar icons.

ii Press ↵. The map shifts to display the first object that matches the search criterion.

iii Press F3 to shift the map focus to the next matching object, if the search finds multiple matches.

iv Press CTRL-F3 to shift the map focus to the previous matching object, if the search finds multiple matches.

v Go to step 5.

3 Click on the OK button.

a If a match is found, the map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

b If multiple matches are found, the Find Object form opens with a drop-down list of all of the search results. Go to step 4.

4 Select a network object and click on the OK button. The map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

5 Manage the object, as required.

Procedure 5-25 To create a bookmark

See section 5.1 for more information about the bookmark function.

1 Open a map.

2 Locate the topology group that you want to bookmark.

> **Note —** Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.

3 Click on the Bookmarks button and choose Add Bookmark. A bookmark for the currently displayed topology group is created.

Procedure 5-26 To manage bookmarks

See section 5.1 for more information about the bookmark function.

1 Open a map, as described in Procedures 5-1 to 5-6.

> **Note —** Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.
>
> Bookmarks that were not created in the map view currently displayed, or that are invalid, are disabled and cannot be selected. In the Manage Bookmarks form, these bookmarks appear in italics.

2 Click on the Bookmarks button and choose Manage Bookmarks. The Manage Bookmarks form opens.

3 Perform one of the following:

- **a** Create a top-level folder to manage the bookmarks.
  - **i** Click on the New Folder button. The Folder Properties form opens.
  - **ii** Enter the name of the new folder in the Name field and click on the OK button. A new top-level folder is added to the list panel.
- **b** Create a folder in an existing folder.
  - **i** Select an existing folder in the list panel and click on the New Folder button. The Folder Properties form opens.
  - **ii** Enter the name of the new folder in the Name field and click on the OK button. A new folder is added to the list panel inside the existing folder.

c Organize your bookmarks and folders. Drag and drop bookmarks and folders in and out of other folders in the list panel.

d Rename a bookmark or folder.

i Select an existing bookmark or folder in the list panel and click on the Rename button. The Rename form opens with the existing name in the Name field.

ii Change the text in the Name field and click on the OK button. The name of the bookmark or folder is modified.

e Delete a bookmark or folder.

i Select a bookmark or folder that you want to delete in the list panel.

ii Click on the Delete button. The selected bookmark or folder is removed from the list panel and the bookmark drop-down menu on the map toolbar.

4 Click on the Close button to close the Manage Bookmarks form and save the changes.

Procedure 5-27 To change the map background image

To view the map background image examples provided by the 5620 SAM, navigate to the background directory in the 5620 SAM client Installation directory, for example, /nms/images/map/background.

When adding your own map image to the directory, ensure that the file type is GIF and that the size is a maximum of 2000 × 2000 pixels.

The default background image is defaultBackgroundImage.gif.

1 Open a map, as described in Procedures 5-1 to 5-6.

2 In the map navigation tree, right-click on the topology group for which you want to change the map background image and choose Properties from the contextual menu. The Group - Network (Edit) form opens.

3 Modify the Background Image parameter to specify a new map image file, for example, n_america.gif.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button to proceed. The background image for the topology group changes to the selected image.

5.7 5620 SAM map management procedures

Use the following procedures to perform map management tasks.

Procedure 5-28 To use OAM diagnostic functions on a service topology map

Perform this procedure to enable the OAM diagnostic functions on a service topology map and use the basic OAM controls in the map window. See the other procedures in this chapter for information about using specific elements such as the toolbar buttons and info tables.

1 Create a service topology map by selecting the service in the Manage Services form and clicking on the Topology View button.

2 Select the OAM check box at the bottom left of the map window.

3 To manage one or more objects, select the objects and right-click on the set of objects to choose an option from the contextual menu.

4 To select a MEG to display, choose the MEG using the drop-down list of available MEGs at the bottom of the map window.

5 To view the properties of the selected MEG, click on the MEG Properties button at the bottom of the window. The Global Maintenance Entity Group (Edit) form opens with the General tab displayed. The service displayed on the map is listed on the Service tab.

6 To resynchronize the MIPs in the selected MEG, click on the Resync MIPs button at the bottom of the window.

7 Use the other procedures in this chapter to refine the map contents or display object properties, as required.

8 Use the right-click contextual menu options to configure and manage OAM objects, as required. See “Managing OAM diagnostics from the topology view” in section 5.1 for a functional description of the available contextual menu options for OAM diagnostics.

Procedure 5-29 To create a topology group

Note — A topology group can contain a maximum of 500 NEs.

1 Open the Group (Create) form using one of the following methods.

a Choose Create→Equipment→Group from the 5620 SAM main menu.

b Right-click on the Network icon in the equipment view of the navigation tree and choose Equipment→Create Group from the contextual menu.

2 Configure the parameters:

- Name
- Description
- Background Image

3 Click on the Apply button.

4 Click on the Spans tab button.

5 Click on the Add button. The Select Span(s) - Equipment Group form opens with a list of available spans.

6 Select one or more spans to apply to the topology group.

7 Click on the OK button. The Select Span(s) - Equipment Group form closes and a dialog box appears.

8 Click on the OK button to confirm the action.

After the topology group is created, an object for the topology group is displayed in the equipment navigation tree, and on the appropriate topology maps.

Procedure 5-30 To populate a topology group

Note — A topology group can contain a maximum of 500 NEs.

1 Choose Application→Physical Topology, or Service Tunnel Topology from the 5620 SAM main menu. The appropriate map window opens.

2 Populate topology groups, as required,

a Click on a map object in the map panel, for example, a router or router group, and drag the object onto the topology group object to which you want the map object to belong in the:

- map panel
- map navigation tree

The map object becomes a descendant object of the topology group.

b Click on a topology group object in the map navigation tree and drag the object onto another group object in the map navigation tree to which you want the group object to belong. The topology group object becomes a descendant object of another group object.

Procedure 5-31 To modify a topology group and create topology groups with the same parameter settings

1. Right-click on the topology group object on the map for which you want to modify the parameters and choose Properties from the contextual menu. The Group (Edit) form opens.
2. Modify the parameters as required.
3. Click on the Apply button. A dialog box appears.
4. Click on the Yes button to save the changes.
5. If required, click on the Copy button to create more topology groups based on the same parameter information. A Group (Create) form opens with the existing parameter information.
6. Edit the parameter information as required.
7. Click on the OK button. The Group (Create) form closes.
8. Close the Group (Edit) form.

   Any changes to the properties of a topology group appear immediately on the equipment navigation tree and the appropriate topology maps.

Procedure 5-32 To delete a topology group

When you delete a topology group object, the topology group cannot contain any devices or descendant topology groups.

1. Choose Application→Physical Topology, or Service Tunnel Topology from the 5620 SAM main menu. The appropriate map window opens.
2. Drag and drop all devices and descendant topology groups from the topology group that you want to delete to another topology group or the root group, for example, the network.
3. Right-click on the topology group object that you want to delete on the map and choose Delete from the contextual menu. A dialog box appears.
4. Click on the Yes button to proceed. The topology group is deleted.

Procedure 5-33 To modify a service or composite service using the topology view

You can use the service or composite service topology view to add, modify, or navigate to service components. The service configuration form can also be accessed directly at any time from this view by right-clicking any component. This allows quick access to conduct more detailed component configuration.

1 Perform one of the following.

  a Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

  b Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure a search filter, if required, and click on the Search button. A list of services or composite services is displayed.

3 Perform one of the following.

  a Select a service and click on the Topology View button. The Service Topology map opens.

  b Select a composite service and click on the Flat Topology View button. The Composite Service Flat Topology View map opens.

4 Right-click on the map background, or on one or more selected service sites, to display a contextual menu of configuration options. When you choose an option, a configuration form opens.

5 See the appropriate service management chapter for information about modifying a specific service type.

Procedure 5-34 To create a physical link

The MDA type for both physical link endpoints must be the same. Only one physical link can be configured on a port.

Users with Device Mgmt privileges can create, modify, and delete physical links.

1 Open the Physical Link (Create) form using one of the following methods.

  a Choose Create→Equipment→Physical Link from the 5620 SAM main menu.

  b Right-click on the topology map background in the equipment view of the navigation tree and choose Equipment→Physical Link from the contextual menu.

2 Configure the parameters:

- Name
- Description
- Endpoint A Type
- Endpoint B Type
- Notes

3 Configure the parameters in the Endpoint A panel by performing one of the following.

a If you set the Endpoint A Type parameter in step 2 to Port, go to step 4.

b If you set the Endpoint A Type parameter in step 2 to Network Element, go to step 5.

c If you set the Endpoint A Type parameter in step 2 to LAG, go to step 6.

4 Configure the parameters in the Endpoint A - Port panel by performing one of the following steps.

a Use the Select Endpoint A - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A – Port panel to choose a managed endpoint for the physical link. The Select Endpoint A - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint A - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint A - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint A - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint A - Port panel.

5 Configure the parameters in the Endpoint A - Network Element panel by performing one of the following steps.

- **a** Use the Select Endpoint A - Network Element - Physical Link form to search for a port.
  - **i** Click on the Select button in the Endpoint A panel to choose a managed endpoint for the physical link. The Select Endpoint A - Network Element - Physical Link form opens.
  - **ii** Use the configurable filter and click on the Search button to generate a list of NEs.
  - **iii** Select an NE and click on the OK button. The Select Endpoint A - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint A - Network Element panel of the Physical Link (Create) form.
- **b** Choose an NE from the equipment navigation tree:
  - **i** Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.
  - **ii** Click on the Paste from Clipboard button in the Endpoint A - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint A - Network Element panel.

6 Configure the parameters in the Endpoint A - LAG panel by performing one of the following steps.

- **a** Use the Select Endpoint A - LAG - Physical Link form to search for a port.
  - **i** Click on the Select button in the Endpoint A panel to choose a managed endpoint for the physical link. The Select Endpoint A - LAG - Physical Link form opens.
  - **ii** Use the configurable filter and click on the Search button to generate a list of NEs.
  - **iii** Select an NE and click on the OK button. The Select Endpoint A - LAG - Physical Link form closes and the NE parameter information is displayed in the Endpoint A - LAG panel of the Physical Link (Create) form.
- **b** Choose an NE from the equipment navigation tree:
  - **i** Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.
  - **ii** Click on the Paste from Clipboard button in the Endpoint A - LAG panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint A - LAG panel.

7 Configure the parameters in the Endpoint B panel by performing one of the following.

a If you set the Endpoint B Type parameter in step 2 to Port, go to step 8.

b If you set the Endpoint B Type parameter in step 2 to Network Element, go to step 9.

c If you set the Endpoint B Type parameter in step 2 to Unmanaged NE, go to step 11.

d If you set the Endpoint B Type parameter in step 2 to LAG, go to step 12.

8 Configure the parameters in the Endpoint B - Port panel by performing one of the following.

a Use the Select Endpoint B - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint B panel to choose a managed endpoint for the physical link. The Select Endpoint B - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint B - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint B - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint B - Port panel.

9 Configure the parameters in the Endpoint B - Network Element panel by performing one of the following.

a Use the Select Endpoint B - Network Element - Physical Link form to search for a port.

i Click on the Select button to choose a managed endpoint for the physical link. The Select Endpoint B - Network Element - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint B - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint B - Network Element panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint B - Network Element panel.

10 If the Endpoint B is an unmanaged NE that the 5620 SAM recognizes as an unmanaged mobile NE such as an eNodeB, go to step 14.

11 Configure the parameters in the Endpoint B - Unmanaged NE panel:

- Unmanaged - Name
- Unmanaged - Management Address
- Unmanaged - Description

Note — If the 5620 SAM is to manage endpoint B, configure the Unmanaged - Name parameter with the management IP address of the unmanaged NE.

When the 5620 SAM discovers the NE, the unmanaged endpoint of the physical link is updated with the newly managed NE on the topology map.

12 Configure the parameters in the Endpoint B - LAG panel by performing one of the following.

a Use the Select Endpoint B - LAG - Physical Link form to search for a port.

i Click on the Select button in the Endpoint B panel to choose a managed endpoint for the physical link. The Select Endpoint B - LAG - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint B - LAG - Physical Link form closes and the port parameter information is displayed in the Endpoint B - LAG panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

ii Click on the Paste from Clipboard button in the Endpoint B - LAG panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint B - Port panel.

13 Go to step 17.

14 Click on the Select button in the Endpoint B - Unmanaged NE (LTE) panel to choose an unmanaged mobile NE such as an eNodeB. The Select Unmanaged NE - Physical Link form opens.

15 Use the configurable filter and click on the Search button to generate a list of unmanaged mobile NEs for example, eNodeBs.

16 Select an unmanaged mobile NE and click on the OK button. The Select Unmanaged NE - Physical Link form closes and the NE information is displayed in the Endpoint B - Unmanaged NE (LTE) panel of the Physical Link (Create) form.

17 Click on the OK button to close the form. The physical link is created between the two endpoints and can be viewed from the physical topology map.

Procedure 5-35 To modify a physical link and create physical links with the same parameter settings

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Modify the parameters as required.

6 Click on the Apply button to save the changes.

7 If required, click on the More Actions button and choose Copy to create more physical links based on the same parameter information. A Physical Link (Create) form opens with the existing parameter information.

8 Edit the parameter information as required.

9 Click on the OK button. The Physical Link (Create) form closes.

10 Close the Physical Link (Edit) form.

After a physical link is created, you can view the link on the physical topology map.

Procedure 5-36 To delete a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Delete button. A dialog box appears.

5 Click on the Yes button to proceed. The physical link is deleted.

Note — When a NE is unmanaged or removed, all the physical links that terminate on the ports or on the NE itself are deleted.

Procedure 5-37 To configure bandwidth availability on physical links

Use this procedure to configure bandwidth parameters on links being used by service CAC.

Note — This capability is only available if service CAC has been configured. See chapter 6 for information about enabling and disabling service CAC.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Perform one of the following.

  a Choose Discovered Physical Link from the object drop-down menu.

  b Choose Physical Link from the object drop-down menu.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Click on the Bandwidth tab button.

6 Select the Endpoint A or the Endpoint B tab.

7 Configure the following endpoint bandwidth parameters:

- Bandwidth (%)
- Used Bandwidth (Mbps)
- Utilization Threshold (%)

8 Configure the following effective bandwidth parameters:

- Name
- Bandwidth (Mbps)
- Booking Factor (%)
- Utilization Threshold (%)
- Used Bandwidth (Mbps)

9 To view a summary of bandwidth usage for all tunnels and services currently using the physical link, click on the Bandwidth Usage tab button.

10 Click on the OK button. The Physical Link (Edit) form closes.

11 Close the Manage Equipment form.

Procedure 5-38 To view and modify discovered physical link properties

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Discovered Physical Link from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button.

4 Select a discovered physical link in the list and click on the Properties button. The Discovered Physical Link (Edit) form opens with the General tab displayed.

5 Configure the following parameters, if required:

- Name
- Description

6 Perform one of the following to configure the link reference information, if required.

a Click on the More Actions button and choose Reference Discovered Links. The parameters in the Reference panel are populated with reference information.

b Click on the More Actions button and choose Clear Reference. The parameters in the Reference panel are reset.

7 Select the appropriate tab to view other information, as required..

8 Click on the OK button. The Discovered Physical Link (Edit) form closes.

9 Close the Manage Equipment form.

Procedure 5-39 To switch between a backup/standby link to an inservice link

1 In the Physical topology map, click on the Protected link between two nodes which is indicated in blue.

2 Right-click on the blue link and select Expand Group, the links are expanded into the Backup/Standby link which is represented in blue and the In Service link which is represented in green.

3 To switch between the links and make the Standby/Backup node In Service and vice versa, click on the relevant Port/Card and right-click and select Properties, the Physical Port (Edit) form opens.

4 Click on the Protection tab button and from the Equipment Protection Scheme Parameter and the Receiver Protection Scheme Parameter, select the Commands option. See Procedures 19-19 and 20-31 for more information on how to set the forced and lockout parameter from the commands option.

5 Click on the Apply button, a dialog box is displayed, confirm the change by selecting Yes.

6 Click on the Cancel button. The Physical Port (Edit) form closes.

5620 SAM system management

6 — 5620 SAM component configuration

6.1 5620 SAM component configuration overview

A 5620 SAM system may occasionally require a configuration change. The procedures in this chapter describe how to perform operations such as the following on the components in a 5620 SAM system:

- changing a component IP address or hostname
- adding a 5620 SAM database, server, or client
- updating a license key to accommodate new software modules or equipment
- changing the configuration of all 5620 SAM GUI clients
- implementing secure communication in a 5620 SAM cluster

Note 1 — You can also change the configuration of a 5620 SAM component such as a database, server, or client using the 5620 SAM installation software, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Note 2 — This chapter does not describe how to configure SSL on a 5620 SAM component. See chapter 10 for information about configuring 5620 SAM SSL.

You can use the 5620 SAM auto-client update function to reconfigure multiple 5620 SAM clients. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about using auto-client update to perform a client update. See Procedure 6-9 for information about performing global auto-client updates.

6.2 Software configuration procedures

The following procedures describe how to view and change the general 5620 SAM software configuration.

Procedure 6-1 To view the 5620 SAM software release and license key information

Perform this procedure to display information about the installed 5620 SAM software release and license capacity.

1 Perform one of the following.

a View the software release information; perform the following steps.

i Choose Help→About 5620 SAM from the 5620 SAM main menu. The About the 5620 SAM Client Application form opens.

ii Review the software release information. The build information specifies the release of the 5620 SAM software installed, for example, Release 8.0 R1, where 8.0 is the major release identifier, and R1 is the minor release identifier.

b View the 5620 SAM license information; perform the following steps.

i Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.

ii Review the software license information, which includes the following:

- active license key value
- hostname and IP address of the main server
- number of supported operator positions
- status of the primary and standby servers
- supported 5620 SAM modules and packages
- redundancy configuration information for redundant deployments

iii Click on the Devices and Quantities Licensed tab button.

iv Review the software license information, which includes the following:

- device information that includes the following:
  - quantity licensed
  - quantity consumed
  - quantity remaining
- card and daughter card information that includes the following:
  - quantity licensed
  - quantity consumed
  - quantity remaining

Note — A highlighted entry is alarmed. You can double-click on an alarmed entry to view the alarm details.

2 Close the open forms.

Procedure 6-2 To export license information to a file

You can export the license information as text to a file storage location. This text file can be sent to Alcatel-Lucent to provide information about your system.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2 Click on the Export License information to file button. A Save as form opens.

3 Use the form to specify a name, location, and format for the file that contains the exported license information.

Note — License key files can be saved in HTML or text format.

4 Click on the Save button. The license key file is saved to the specified location.

5 Close the 5620 SAM License (Edit) form.

Procedure 6-3 To verify that the required 5620 SAM software modules are installed

The 5620 SAM functions are provided by the following modules that are enabled or disabled using the 5620 SAM license key:

- 5620 SAM-A—for OAM tools, service assurance functions, fault correlation using alarms, topology views, and statistics management
- 5620 SAM-E—for device mediation, equipment navigation and management, security, CLI access, backup and restore, alarm management, real-time equipment statistics, and inventory and reporting
- 5620 SAM-O—for the 3GPP and XML open interfaces
- 5620 SAM-P—for service provisioning, templates, and management of network customers, subscribers, tunnels, paths, and policies
- Mobile Services Package—for LTE functions

Note — The 5620 SAM-E module is enabled By default. You cannot install and run other modules without installing the 5620 SAM-E.

If a module or package is not installed, you cannot use the client GUI to perform the functions associated with the module or package.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.

2 View the options in the 5620 SAM Modules and Packages Licensed panel. If a module or package is not selected, it is not enabled in the license key.

3 Verify that the required software modules are installed.

If you cannot perform a function using the client GUI and you have sufficient user privileges on a managed device, you can use a CLI on the device to perform the function.

4 View the other license key information, as required.

5 Close the 5620 SAM License (Edit) form.

Procedure 6-4 To change the license key in a standalone 5620 SAM system

Perform this procedure to update the 5620 SAM license information for a standalone 5620 SAM system.

A 5620 SAM license key is generated based on multiple parameters such as the platform type, the software release, and the required number of GUI clients and managed MDAs. When a license key parameter changes, a new license key is required.

Note — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

6 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

```
key="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXX
```

XX-XXXXX-XXXXX-XXXXX"

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the functions defined in the updated license key are enabled.

11 Enter the following at the prompt:

```
bash$ ./nmsserver.bash nms_status ↵
```

The main server displays status information.

12 Review the information in the 5620 SAM License Information section of the command output to ensure that it is correct.

13 If one or more license parameters are incorrect, contact Alcatel-Lucent technical support for assistance.

Procedure 6-5 To change the license key in a redundant 5620 SAM system

Perform this procedure to update the 5620 SAM license information for a redundant 5620 SAM system.

A 5620 SAM license key is generated based on multiple parameters such as the platform type, the software release, and the required number of GUI clients and managed MDAs. When a license key parameter changes, a new license key is required.

In a redundant 5620 SAM system, the primary and standby main server license key parameters must be identical, except for the primary and standby main server station host IDs.

Caution — The primary and standby main server license keys must be synchronized to ensure proper 5620 SAM operation in the event of a main server activity switch. The main servers compare license key values when they establish communication or when one main server is performing a read_config operation using the nmsserver.bash script. If a difference in the keys is detected, the 5620 SAM raises an alarm that clears when the license keys are again synchronized.

Note — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

Change license key on primary main server

1 Log in to the primary main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

6 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

```
key="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXX
XX-XXXXX-XXXXX-XXXXX"
```

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file, the license information is updated, and the additional functionality defined in the updated license key is enabled.

11 Enter the following at the prompt to verify the updated license information:

```
bash$ ./nmsserver.bash nms_status ↵
```

The main server displays status information.

12 Review the 5620 SAM License Information section of the command output to ensure that the license parameters are correct.

Note — The license information that is displayed is associated with the local main server.

13 Keep the console window open. It is used later in the procedure.

Change license key on standby main server

14 Log in to the standby main server station as the samadmin user.

15 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

16 Create a backup copy of the nms-server.xml file.

17 Open the nms-server.xml file using a plain-text editor.

18 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

19 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

```
key="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXX
XX-XXXXX-XXXXX-XXXXX"
```

20 Save and close the nms-server.xml file.

21 Open a console window.

22 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

23 Enter the following at the prompt:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts using the updated license information, and the additional functionality defined in the updated license key is enabled.

24 Enter the following at the prompt to verify the updated license information:

```
bash$ ./nmsserver.bash nms_status ↵
```

The main server displays status information.

25 Review the 5620 SAM License Information section of the command output to ensure that the license parameters are correct.

Note — The license information that is displayed is associated with the local main server.

26 Compare the standby main server license information to the active main server information displayed in step 12 to ensure that it is the same.

27 If the active and standby license parameters do not match, contact Alcatel-Lucent technical support for assistance.

Procedure 6-6 To change the timed license expiry notice period

The 5620 SAM raises a daily warning alarm as the expiry date of the 5620 SAM license key approaches. By default, the first daily warning alarm will be raised seven days prior to the key expiry date. This value is configurable. Perform this procedure to change the number of days.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<license
```

```
timedLicenseExpiryCount="value"
```

where *value* is the number of days prior to timed license key expiry.

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the time period defined is updated.

Procedure 6-7 To configure the maximum number of 5620 SAM admin user sessions

Perform this procedure to configure the maximum number of 5620 SAM admin user sessions that can be active concurrenly.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<samsession
```

This section of the file contains the maximum number of admin sessions that can be configured.

max5620SAMAdminSessions="value"

where *value* is the max number of allowed admin user sessions.

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the number of sessions defined.

10 Log out of the main server.

11 Close the open console windows, as required.

Procedure 6-8 To enable 5670 RAM support

Perform this procedure to enable the 5670 RAM functions on a 5620 SAM system. You require samadmin user privileges to perform this procedure.

1 If the 5620 SAM is deployed in a standalone configuration, go to step 5.

2 Perform steps 5 to 15 on the primary main server.

3 Perform steps 5 to 15 on the standby main server.

4 Go to step 16.

5 Log in to the main server station as the samadmin user.

6 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

7 Create a backup copy of the nms-server.xml file.

8 Open the nms-server.xml file using a plain-text editor.

9 Locate the following section:

```
<ram5670
        ramEnabled="false" />
```

10 Change “false” to “true”.

11 Save and close the nms-server.xml file.

12 Open a console window.

13 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

14 Perform one of the following:

a If you are configuring a standalone main server, or the primary main server in a redundant deployment, enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and puts the configuration change into effect.

b If you are configuring the standby main server in a redundant deployment, enter the following at the prompt:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

15 Log out of the main server.

16 Close the open console windows, as required.

6.3 System configuration procedures

The following procedures describe how to configure system parameters that define the connections between 5620 SAM components.

Procedure 6-9 To change the global 5620 SAM client configuration using the auto-client update utility

Perform this procedure to modify the base configuration of each 5620 SAM GUI client that connects to a specific 5620 SAM main server.

Note 1 — You can exclude a specific 5620 SAM client from a global configuration change by using a command-line option when you open the client GUI, as described in chapter 3.

Note 2 — Do not use this procedure to configure SSL for 5620 SAM clients. Use the appropriate SSL configuration procedures in chapter 10 to configure SSL.

Note 3 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Modify the appropriate client configuration file in the *install_dir*/nms/config/clientDeploy directory with the configuration change. For example, update the nms-client.xml file with a new client log location.

where *install_dir* is the server installation location, typically /opt/5620sam/server

3 Open a console window.

4 Enter the following at the prompt to enable an update notification for clients that connect to the server and to prepare the client configuration files for download.

bash$ ***install_dir*/bin/nmsdeploytool.bash deploy** ↵

where *install_dir* is the server installation location, typically /opt/5620sam/server

5 Perform one of the following on each 5620 SAM single-user GUI client station and client delegate server station.

Note — When you perform this step on a client delegate server, you affect each GUI client that connects through the client delegate server.

a Update the client configuration by restarting the client GUI. The client automatically backs up the current configuration and applies the configuration change.

Note — On a client delegate server station, you must start the client software as the root user or the configuration update fails.

A Solaris client stores the backup of the current configuration in the *install_dir*/nms/configBackup directory

where *install_dir* is the client installation location, typically /opt/5620sam/client

A Windows client stores the backup of the current configuration in the *install_dir*\nms\configBackup directory

where *install_dir* is the client installation location, typically C:\5620sam\client

b Preserve the current client configuration when the client GUI starts by specifying a startup option that disables the auto-client update function. See chapter 3 for information about 5620 SAM client startup options.

Note — Specifying a client startup option affects only the current GUI session. To ensure that the client configuration is not updated automatically during a subsequent session, you must open the session using the startup option that disables the auto-client update.

Procedure 6-10 To configure a client GUI login form to display multiple server options

Perform this procedure to enable the users of a specific 5620 SAM client GUI to choose the 5620 SAM main server to which they connect.

Note 1 — You cannot configure a client delegate server to display multiple server options on the client login form. If you require client connections to multiple 5620 SAM servers through a client delegate server, you must install one 5620 SAM client delegate software instance for each 5620 SAM server.

Note 2 — The 5620 SAM auto-client update function overrides the nms-client.xml configuration changes that are specified in this procedure. If the nms-client.xml file on a main server changes, it overwrites the local client copy the next time the client connects to the server, unless a client startup option is used to prevent it. For information about using client startup options, see chapter 3.

Alcatel-Lucent recommends that you use the 5620 SAM auto-client update function described in chapter 6 to modify the 5620 SAM client configuration.

1 Click on Application→Exit to close the 5620 SAM client GUI, if it is open. The client GUI closes.

2 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

3 Open the nms-client.xml file using a text editor.

4 Find the lines starting with <j2ee> and <systemMode>. By default, the IP address and port information of the standalone or redundant servers, as configured during installation, are displayed.

5 For each standalone main server or redundant main server pair you want displayed on the client GUI login form, perform the following:

i Copy the entire <j2ee> and <systemMode> sections of the file.

ii Paste the <j2ee> and <systemMode> sections after the previous section.

iii Modify the ejbServer IP address to the IP address or hostname of the server you want displayed during client GUI login.

iv Modify the nameOne (for standalone) or nameOne and nameTwo (for redundant) parameters to indicate the domain name and hostname of the server, for easier identification by operators. This name does not have to be the hostname of the server domain. In some cases, the name may be the same for the active and standby server in a redundant server domain. The name is not automatically derived from a host lookup.

Note — Common hostname restrictions apply to the nameOne and nameTwo fields. You cannot use the following special characters:

- !
- #
- $
- %
- &
- (
-)
- +

v Save the changes and close the file.

6 Log in to the client GUI. The new server options are displayed in the Server drop-down menu.

Procedure 6-11 To change the default GUI preference and table layout, script result, or log file location on a client delegate server

Perform this procedure to customize the default file location for one or more of the following on a 5620 SAM client delegate server:

- user-defined GUI preferences:
  - saved table layouts
  - preferences saved using Application→Save Workspace
- script result files
- client log files

1 Close each 5620 SAM client that connects to the main server through the client delegate server by choosing Application→Exit from the 5620 SAM main menu.

2 Log in to the client delegate server station as the samadmin user.

3 Open a console window.

4 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config.

5 To change the default saved GUI preferences and table layout file location:

i Open the nms-client.xml file using a plain-text editor.

ii Insert the following section directly above the </configuration> line at the end of the file:

```
<guiPreferences
        path="new_file_location"
    />
```

where *new_file_location* is the new default saved GUI table layout and GUI preferences file location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

iii Save and close the nms-client.xml file. Subsequent 5620 SAM client sessions on the client delegate server save the GUI preferences and table layouts to files in the new location.

6 To change the default script result file location:

i Open the nms-client.xml file using a plain-text editor.

ii Insert the following section directly above the </configuration> line at the end of the file:

```
<cache
        directoryName="new_file_location"
    />
```

where *new_file_location* is the new default script result file location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

iii Save and close the nms-client.xml file. Subsequent 5620 SAM client sessions on the client delegate server save the script results to files in the new location.

Procedure 6-12 To change the IP address or hostname of a 5620 SAM server or database

Perform this procedure to change the IP address or hostname of one or more main server, auxiliary server, or database components in a standalone or redundant 5620 SAM system. This may be required, for example, when the management network topology changes.

Caution — Changing an IP address or hostname in a 5620 SAM system is a complex operation that requires careful planning and organization, and depending on the type of change required, may involve a brief network management outage. Do not attempt to modify the network configuration of a 5620 SAM component without assistance from Alcatel-Lucent technical support.

1 Collect the following information:

- the current IP address or hostname of each main server, auxiliary server, and database in the 5620 SAM system
- the new IP addresses or hostnames that are to be assigned

2 Contact Alcatel-Lucent technical support to schedule a maintenance period for the network configuration change.

Procedure 6-13 To change the IP address of a 5620 SAM client delegate server

Perform this procedure when a client delegate server is assigned a new IP address.

1 Collect the following information:

- the current IP address or hostname of the client delegate server
- the new IP address or hostname of the client delegate server

2 Contact Alcatel-Lucent technical support to schedule a maintenance period for the network configuration change.

Procedure 6-14 To enable 5620 SAM database backup file synchronization

Perform this procedure to enable the main servers in a redundant 5620 SAM deployment to synchronize the database backup file sets. After a database backup, if database backup file synchronization is enabled, the 5620 SAM automatically copies the new database backup file set to the other database station.

Note 1 — This procedure applies only to redundant 5620 SAM deployments.

Note 2 — You must perform this procedure first on the standby main server station, and then on the primary main server station.

Note 3 — Before you perform this procedure, you must ensure that there is sufficient network bandwidth between the database stations for a database copy operation. See the *5620 SAM Planning Guide* for information about the bandwidth requirements of database backup file synchronization.

1 Log in to the main server station as the root user.

2 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

3 Open a console window.

4 Perform one of the following to open the 5620 SAM server installer.

a On a SPARC station:

i Enter the following:

\# **cd Solaris** ↵

ii Enter the following:

\# **./ServerInstall_SAM_9_0_*revision*.bin** ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On an x86-based station:

i Enter the following:

\# **cd Solarisx86** ↵

ii Enter the following:

\# **./ServerInstall_x86_SAM_9_0_*revision*.bin** ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

5 Click on the Next button.

6 Accept the terms of the license agreement in the “Software License Agreement” panel.

7 Click on the Next button.

8 Choose Main Server Configuration in the “Choose Installation Type” panel.

9 Click on the Next button.

10 Click on the Next button in each subsequent panel until the “Standby Database Configuration” panel is displayed.

11 Select the “Enable Database Backup File Synchronization” parameter.

12 Click on the Next button.

13 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

14 Click on the Done button to close the server configuration utility.

15 Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

16 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

17 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration changes into effect. The 5620 SAM automatically copies subsequent database backup file sets from the primary database station to the standby database station.

Procedure 6-15 To change the Statistics Browser default Past number of hours filter

Due to the large number of statistics that can be stored in the 5620 SAM database, filters should be used when performing statistic searches to limit the search results to the time period. By default, the Statistics Browser form applies a filter to limit the search results to the past one hour. The number of hours is configurable. Perform this procedure to configure the Past <number_of_hours> filter, found on the Browse Statistics form, to limit the number of statistics listed.

1 Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.

2 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

3 Open the nms-client.xml file using a text editor.

4 Locate the XML tag:

```
<statistics
```

5 Edit the following line to read:

```
browserDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter.

6 Save the changes and close the file.

7 Launch a new 5620 SAM client and login. The new value is displayed on the Browse Statistics form.

Procedure 6-16 To change the Statistics tab default Past number of hours filter

Perform this procedure to configure the Past <number_of_hours> filter, found on the Statistics tab of the object form.

1 Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.

2 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

3 Open the nms-client.xml file using a text editor.

4 Locate the XML tag:

```
<statistics
```

5 Edit the following line to read:

```
tabDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter.

6 Save the changes and close the file.

7 Launch a new 5620 SAM client and login. The new value is displayed on the Statistics tab of the object properties form.

6.4 Network management configuration procedures

The following procedures describe how to configure system-wide 5620 SAM functions related to the managed network.

Procedure 6-17 To change the system name of a managed device

Perform this procedure to change the system name of one of the following device types using a 5620 SAM utility:

- 7210 SAS-D 6F 4T
- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

Caution — This procedure requires a restart of a 5620 SAM main server, which is service-affecting. To avoid service interruption in a redundant deployment, schedule the system name change to coincide with a maintenance window and perform this procedure on the 5620 SAM main server. System name changes are automatically propagated to the standby server.

Note 1 — The 5620 SAM main server utility lists other NE types, but does not support changing the system name for devices that are not listed above.

Note 2 — The change can be implemented using SNMPv2c or SNMPv3.

1 Stop the main server software. After this step, the 5620 SAM main server is not managing the network.

i Open a console window.

ii Log in as the samadmin user.

iii Navigate to the server binary directory. Enter the following at the prompt:

```
bash$ cd install_dir/nms/bin ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

iv Enter the following at the prompt:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following at the prompt:

```
bash ./nmsserver.bash appserver_status ↵
```

vi The server application is stopped when the command in step 1 v returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 1 v. Do not proceed unless the console displays the above text.

2 Use a text editor to open the updateSysName.properties file in the current directory.

3 Follow the instructions in the file to update the SNMPv2c or SNMPv3 settings in the file, depending on the SNMP version that the device uses.

4 Save and close the updateSysName.properties file.

5 Enter the following at the prompt to initiate a system name change for the device.

bash$ **./updateSysName.bash** ↵

6 Enter the ID of the device that you want to update.

7 Enter the new system name.

8 Enter the following at the prompt to start the 5620 SAM main server:

bash$ **./nmsserver.bash start** ↵

The main server starts.

Procedure 6-18 To configure the 5620 SAM to save device configuration backups on a file system

Perform this procedure to configure the 5620 SAM to save device configuration backups as files in addition to saving them in the database. By default, the 5620 SAM saves device configuration backups only in the 5620 SAM database.

Note — The samadmin user requires read and write permissions to each directory specified in this procedure.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag, which marks the beginning of the section that you want to configure:

<*device_type*backup

where *device_type* is one of the following:
Ran—for RAN devices such as the eNodeB
AosSr—for OmniSwitch devices
MPRSr—for 9500 MPR devices
sr—for all other devices, such as the 7450 ESS, 7710 SR, and 7750 SR

The same *device_type* identifier is used in the following steps.

6 To enable the storage of device backups on the main server file system, configure the following parameter by inserting the storage location between the quotation marks:

device_type`BackupDirectory="`*location*`"`

where *location* is an absolute or relative file path

Note — A relative file path that you specify in this step is relative to the *installation_directory*/nms/bin directory on the 5620 SAM main server.

7 If required, configure the following parameters by changing the value between the quotation marks:

Note — The default value for each parameter is shown in this step.

`diskUsageThreshold="80"`

`maxNumberOfFiles="5000"`

`purgeDiskUsageThreshold="95"`

`saveLatestOnly="true"`

device_type`BackupSyncEnabled="false"`

device_type`BackupSyncInterval="30"`

The following are the parameter descriptions:

- diskUsageThreshold—The percentage of disk usage above which the 5620 SAM raises a major alarm. When the disk usage falls below this value, the alarm clears. The range is 0 to 95; the default is 80. A value of 0 means that the disk usage is not monitored.
- maxNumberOfFiles—The maximum number of backup files for this device type that are saved on the file system. When this value is exceeded, the 5620 SAM deletes the oldest backup files. The range is 0 to 100 000; the default is 5000. A value of 0 means that no limit is enforced.
- purgeDiskUsageThreshold—The percentage of disk usage above which the 5620 SAM deletes the oldest backup files and raises a major alarm. The files are deleted until the disk usage falls below the percentage specified by diskUsageThreshold. A value of 0 means that no file deletion occurs and, accordingly, no alarm is raised. The range is 0 to 95; the default is 95.
- saveLatestOnly—If set to true, specifies that only the latest device backup is saved. If set to false, specifies that device backups are saved according to the constraints specified by the diskUsageThreshold, maxNumberOfFiles, and purgeDiskUsageThreshold parameters.
- *device_type*BackupSyncEnabled—If set to true, specifies that the 5620 SAM synchronizes the backup files between the primary and standby main servers.
- *device_type*BackupSyncInterval—If *device_type*BackupSyncEnabled is set to true, specifies how often, in m, the 5620 SAM synchronizes the files.

8 To disable the storage of device backups on the main server file system, configure the following parameter by removing the storage location between the quotation marks, as shown in the following example:

```
device_typeBackupDirectory=""
```

9 Perform steps 5 to 8 to configure the storage of device backups for another device type, if required.

10 Save and close the nms-server.xml file.

11 Open a console window.

12 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

13 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration changes into effect. Subsequent device configuration backups are saved to the path specified in the nms-server.xml file.

The 5620 SAM saves the device backup files in the following directory under the location specified in step 5:

`samNodeBackup/`*`device_ID`*`/`*`timestamp`*

where
device_ID is the unique identifier of a device
timestamp is the time when the backup is saved

Procedure 6-19 To configure automatic device configuration backup file removal

Perform this procedure to configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged.

Caution — This procedure requires a restart of the 5620 SAM server, which is service-affecting.

Note — This procedure configures the removal of backup files only; device configuration backups in the database are retained.

1 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

2 Create a backup copy of the nms-server.xml file.

3 Open the nms-server.xml file using a plain-text editor.

4 Search for the following XML tag:

```
</configuration>
```

5 Enter the following line above the </configuration> tag:

```
<nodeBackups removeBackupOnDelete="true"/>
```

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the console prompt to restart the 5620 SAM server:

```
bash$ ./nmsserver.bash force_restart ↵
```

Caution — Restarting a 5620 SAM server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

10 The 5620 SAM main server restarts. The 5620 SAM deletes the configuration backup files of NEs that are subsequently unmanaged.

Procedure 6-20 To configure service CAC

Perform this procedure to configure the service CAC functionality to enable 5620 SAM to automatically bind PBB tunnels to services based on available bandwidth.

Note 1 — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for more information about the availability of this feature.

Note 2 — You must perform this procedure on each main server in a 5620 SAM system.

1 Close each 5620 SAM client that connects to the main server through the client delegate server, by choosing Application→Exit from the 5620 SAM main menu.

2 Use an OS utility to change the IP address of the client delegate server station to the new value.

3 Log in to the main server station as the samadmin user.

4 Open a console window.

5 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

6 Open the nms-server.xml file using a plain-text editor.

7 Locate the following XML tag:

```
<require-CAC
```

The service CAC section should read as follows:

```
<require-CAC

        enabled="false"

        defaultBWThreshold="90"

        linkTunnelCacheMaxSize="1000"

        tunnelServiceCacheMaxSize="10000"
```

```
        serviceBWCacheMaxSize="50000"
    />
```

8 Change enabled="false" to enabled="true".

9 Save and close the nms-server.xml file.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

11 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and enables the server CAC features on the client delegate server.

Procedure 6-21 To enable alarm reporting for duplicate NE system IP addresses

Perform this procedure to enable the 5620 SAM to verify the uniqueness of NE system IP addresses. When verification is enabled, the 5620 SAM raises an alarm when an NE reports a system IP address that is in use by another NE.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following tag that marks the beginning of the SNMP section:

```
<snmp
```

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

```
verifyNodeIdentity=”1"
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and alarm reporting for duplicate NE system IP addresses is enabled.

Procedure 6-22 To enable LSP on-demand resynchronization

Perform this procedure to modify the nms-server.xml file to enable LSP on-demand resynchronization. The 5620 SAM scheduled resynchronization is then disabled for some LSP objects. See chapter 32 for more information.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following line:

```
<lspOnDemand overrideEnabled="false" />
```

6 Change "false" to "true".

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and LSP on-demand resynchronization is enabled.

Procedure 6-23 To enable debug configuration file reloading for mirror services

Perform this procedure to ensure that the managed NEs reload the debug configuration file after an NE restarts. This ensures that the mirror services in the managed network resume operation after a reboot or CPM activity switch on the NE that hosts the mirror service. By default, debug configuration file reloading is disabled.

Caution — This procedure requires a 5620 SAM main server restart, which is service-affecting.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<serviceMirror
```

6 Specify the NE location of the debug configuration file. For example:

```
<serviceMirror
debugFilename=""
reloadDelay="10"
/>
```

where
reloadDelay specifies the time, in seconds, to wait before a reload request is sent
debugFilename specifies the location of the file on an NE, for example, cf3:/ServiceMirror.dbg

Note — The debugFilename value must be the debug configuration filename that is configured on the NEs that host mirror services.

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

Caution — Restarting a 5620 SAM main server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

The main server restarts.

10 If required, create a device backup policy to ensure that device configurations are not lost in the event of an NE failure. See chapter 23 for information about device backup policies.

Procedure 6-24 To create a default SNMPv2 OmniSwitch user on a 5620 SAM system

Perform this procedure to create a default SNMPv2 OmniSwitch user on a 5620 SAM system.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information that is configured in the following steps.

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

snmpV2UserName=”user_name”

where *user_name* is a user name that is configured on the switch

The SNMP section should read as follows:

```
<snmp
            ip="server_IP_address"
            port="port_number"
            trapLogId="log_ID"
            snmpV2UserName="user_name" />
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

bash$ **./nmsserver.bash read_config** ↵

The main server reads the nms-server.xml file and the new SNMPv2 user name is enabled.

7 — 5620 SAM system redundancy

7.1 5620 SAM system redundancy overview

You can deploy a 5620 SAM system in a redundant configuration to provide greater fault tolerance by ensuring that there is no single point of software failure in the 5620 SAM management network. A redundant 5620 SAM deployment consists of the following components:

- primary and standby 5620 SAM main servers
- primary and standby 5620 SAM databases

Note 1 — For conciseness, a primary 5620 SAM main server is sometimes called a primary server in this chapter.

Note 2 — For conciseness, a standby 5620 SAM main server is sometimes called a standby server in this chapter.

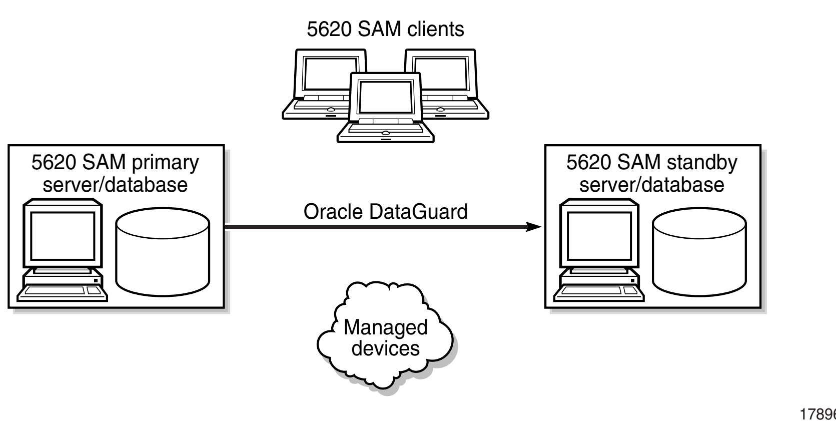
The current state of a component defines the primary or standby role of the component. The primary main server actively manages the network and the primary database is open in read/write mode. When a standby component detects a primary component failure, it automatically changes roles from standby to primary. You can also change the role of a component using the 5620 SAM client GUI or a CLI script.

The 5620 SAM supports collocated and distributed system redundancy. A collocated system requires two stations that each host a main server and database. A distributed system requires four stations that each host a main server or database. Each main server and database is logically independent, regardless of the deployment type.

Caution — For increased 5620 SAM system performance and fault tolerance, Alcatel-Lucent recommends that you deploy the primary server and database in the same geographical location and LAN.

Figure 7-1 shows a collocated redundant 5620 SAM system.

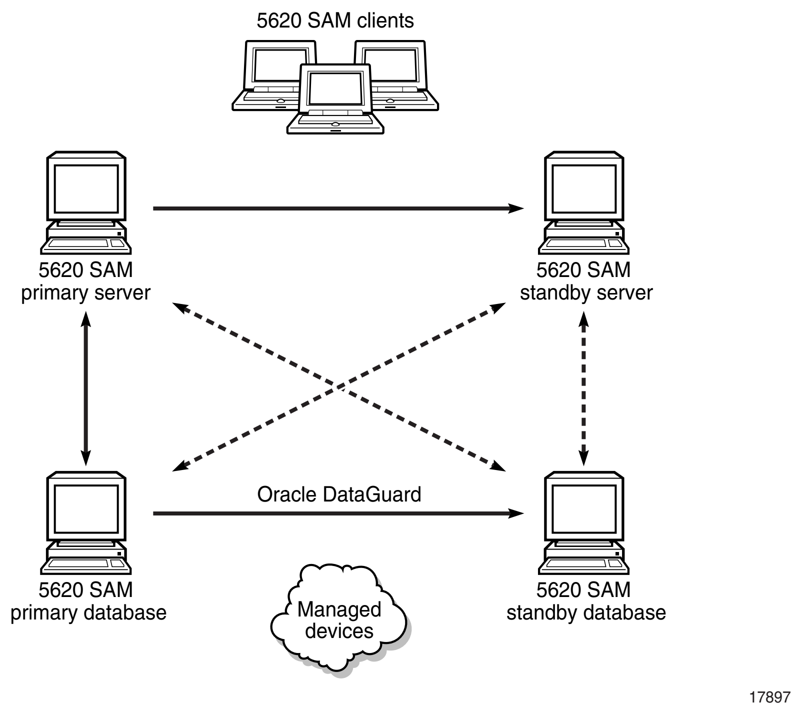
Figure 7-1 Collocated redundant 5620 SAM system



The primary and standby main servers can communicate with the redundant databases, and periodically verify server redundancy. If the standby server fails to reach the primary server within 60s, the standby server becomes the primary server. A 5620 SAM database uses the Oracle DataGuard function to maintain redundancy.

Figure 7-2 shows a distributed redundant 5620 SAM system.

Figure 7-2 Distributed redundant 5620 SAM system



In 5620 SAM redundancy server installation, the Oracle DataGuard synchronization level is set to real-time apply by default to keep the primary and secondary databases synchronized.

A main server role change is called a server activity switch. An automatic database role change is called a failover. A manual database role change is called a switchover.

A typical redundant 5620 SAM deployment has a primary server and database in a facility that is geographically separate from the standby server and database facility. To ensure that the primary components are in the same LAN after an activity switch or failover, you can configure automatic database realignment during 5620 SAM server installation. See “Automatic database realignment” for more information.

The 5620 SAM GUI clients always communicate with the current primary server. After a server activity switch, the GUI clients automatically connect to the new primary server, which is the former standby server. The 5620 SAM OSS clients also communicate with the current primary server, but after a server activity switch, the OSS clients do not automatically connect to the new primary server.

You can use the 5620 SAM GUI, or scripts on a 5620 SAM main server, to do the following:

- Check the redundant server and database status.
- Perform an activity switch from the primary to standby server.
- Reinstantiate the former primary database as the standby database.

5620 SAM system redundancy is configured during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring 5620 SAM redundancy.

The following general conditions apply to 5620 SAM system redundancy:

- The main servers and databases must each be redundant. For example, you cannot have redundant servers and a standalone database.
- The network that contains a redundant 5620 SAM system must meet the latency and bandwidth requirements described in the *5620 SAM Planning Guide*.

  Note — To provide hardware fault tolerance in addition to software redundancy, Alcatel-Lucent recommends using redundant physical links between the primary and standby servers and databases to ensure there is no single point of network or hardware failure.

- The server and database stations require the same OS version and patch level.
- The primary and standby server stations must have identical disk layouts and partitioning.
- The primary and standby database stations must have identical disk layouts and partitioning.
- The following users can perform manual server activity switches or database switchovers:
  - the samadmin user on a main server station
  - a client GUI user that has update or execute access permissions on the db.DatabaseManager.switchover and db.DatabaseManager.reinstantiateStandby classes
  - a client GUI user that has the admin scope of command role

Auxiliary servers

5620 SAM auxiliary servers are optional servers that extend the network management processing engine by distributing server functionality, for example, statistics collection, among multiple stations in a 5620 SAM domain. Each auxiliary server is installed on a separate station in a 5620 SAM server cluster. An auxiliary server communicates only with the primary main server and database. Main and auxiliary servers can open sessions only on the primary database.

A 5620 SAM main server controls task scheduling and sends task requests to auxiliary servers. When a Preferred auxiliary server is unresponsive, the main server directs the requests to a Reserved auxiliary server. The Preferred or Reserved role of an auxiliary server is specified during 5620 SAM main server installation.

When an auxiliary server cannot connect to the primary main server or database, it re-initializes and continues trying to connect until it succeeds or, in the case of a database failover, until the main server directs it to the new database.

An auxiliary server does not cause, perform, or initiate redundancy activities such as failovers. However, an unused, or Reserved, auxiliary server may be called into service by the main server when another auxiliary server fails.

When an auxiliary server fails to respond to the primary main server, the main server tries repeatedly to establish communication before it raises an alarm. The alarm clears when the main server receives a response. 5620 SAM system performance may degrade when a main server loses contact with a number of auxiliary servers that exceeds the number of Preferred auxiliary servers in the 5620 SAM server cluster.

After startup, an auxiliary server waits for initialization information from a main server. An auxiliary server restarts if it does not receive all required initialization information within five minutes.

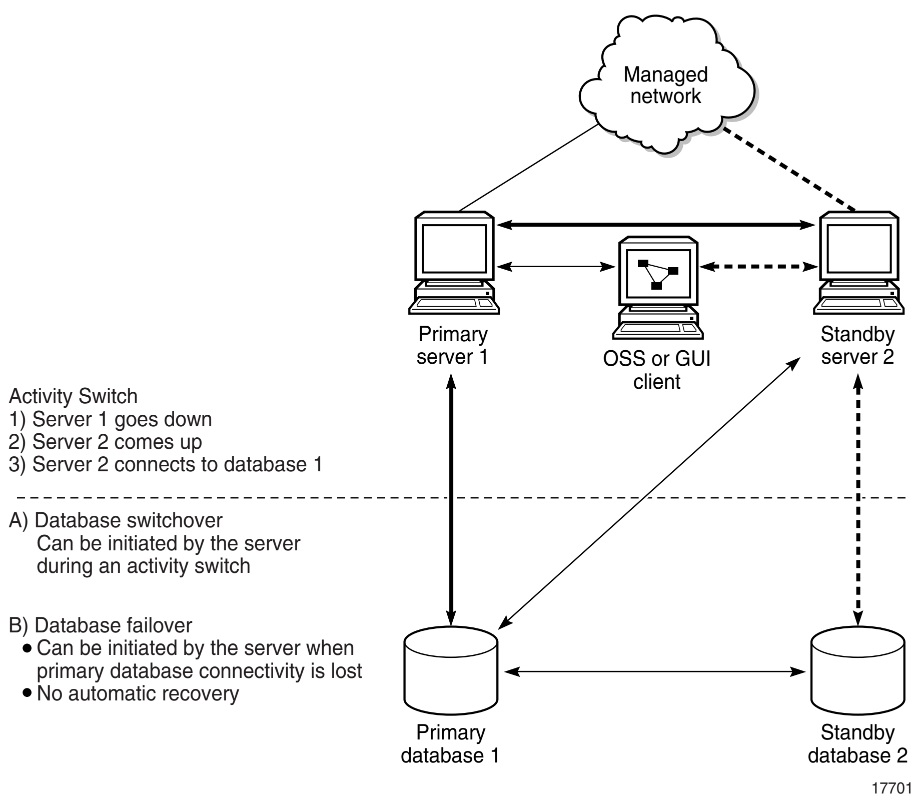
Note — Because an auxiliary server does not play an active role in 5620 SAM redundancy, the unqualified term "server" in this chapter refers to a 5620 SAM main server.

See the *5620 SAM System Architecture Guide* for more information about the interaction of 5620 SAM main and auxiliary servers.

Redundancy functions

Figure 7-3 shows the 5620 SAM system redundancy role-change events.

Figure 7-3 5620 SAM redundancy role-change events

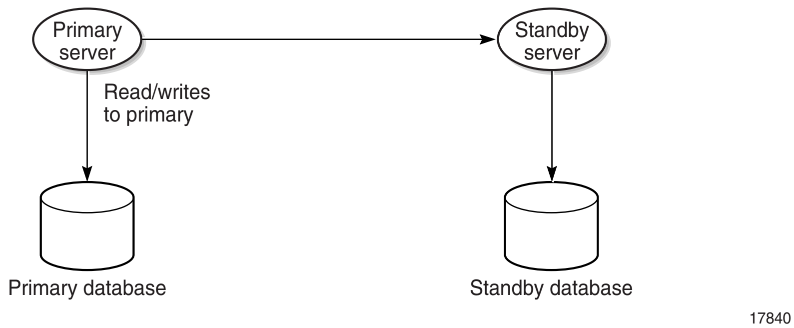


Server activity switches

The standby server initiates an automatic server activity switch when it cannot communicate with the primary server. A 5620 SAM administrator performs a manual server activity switch.

Figure 7-4 shows the server and database roles before an activity switch.

Figure 7-4 Server and database roles before server activity switch



A manual server activity switch is typically a planned server maintenance or testing operation. For security reasons, you cannot use a 5620 SAM GUI or OSS client to perform a server activity switch.

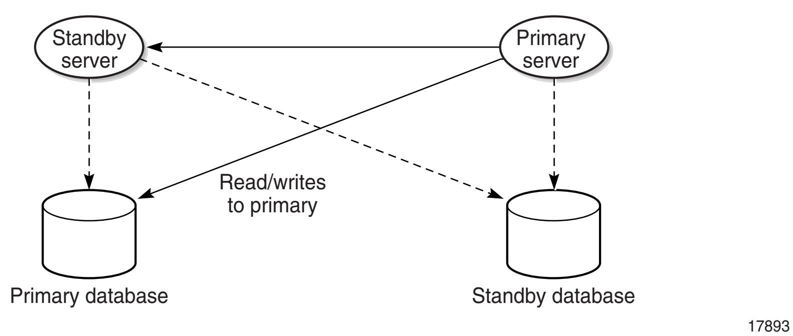
During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics. Auxiliary servers process outstanding requests during an activity switch, but do not communicate with a main server.

The following occurs during a server activity switch:

- The primary server raises alarms about the event.
- Each GUI client receives notification of the activity switch and displays a message about the server unavailability during the activity switch.

Figure 7-5 shows the server and database roles after a successful activity switch.

Figure 7-5 Server and database roles after server activity switch



The following occurs after a server activity switch:

- If automatic database realignment is enabled, the new primary server performs a database switchover.
- The GUI clients communicate with the new primary server and display the current redundancy status.
- The OSS clients must connect to the new primary server, as described in the *5620 SAM XML OSS Interface Developer Guide*.
- The new primary server establishes communication and synchronizes information with the 5620 SAM auxiliary servers.
- The auxiliary servers exchange information with the new primary server; no auxiliary servers exchange information with the former primary server.
- The Preferred or Reserved state of each auxiliary server changes, depending on the configuration of the new primary server.
- The new primary server attempts to redeploy the client requests that the former primary server did not complete before the activity switch.

The connected 5620 SAM GUI clients do not need to re-login if there is a failover or switchover of the server of database. During the failover or switchover, there may be inactivity for the connected clients, but when the new primary server and database are established, all connected user sessions will be seamlessly transferred to the new servers.

Database switchovers

A 5620 SAM administrator directs a main server to initiate a database switchover. Figure 7-6 shows the main server and database roles before a database switchover.

Figure 7-6 Server and database roles before database switchover

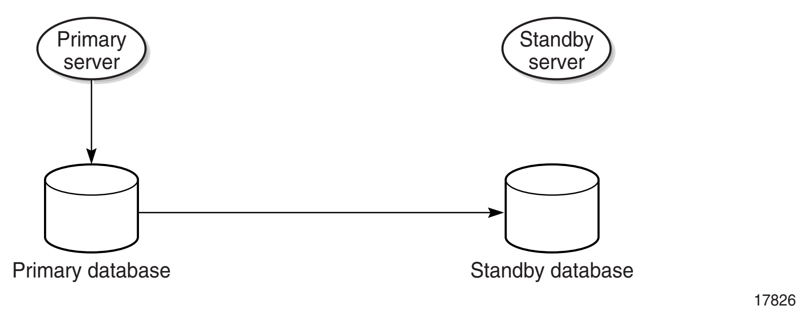
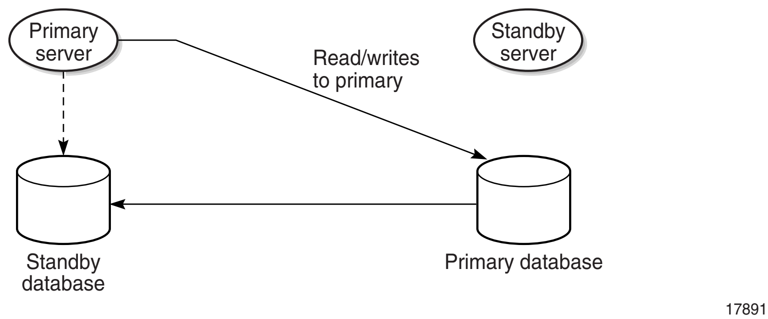


Figure 7-7 shows the server and database roles after a database switchover.

Figure 7-7 Server and database roles after database switchover



The following occurs after a successful database switchover:

- The primary server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary server directs each auxiliary server to use the new primary database.

When a database switchover fails, the primary and standby database roles do not change. No automatic database realignment occurs as a result of a switchover.

Database failovers

5620 SAM database failover functionality is enabled by default. A failover occurs when a main server cannot communicate with the primary database, but can communicate with the standby database and the managed NEs. When this happens, the main server directs the standby database to become the primary database.

A database failover occurs only under the following conditions.

- The standby database is configured, operational, and reachable.
- The main server can communicate with the managed NEs.

Figure 7-8 shows the server and database roles before a failover.

Figure 7-8 Server and database roles before database failover

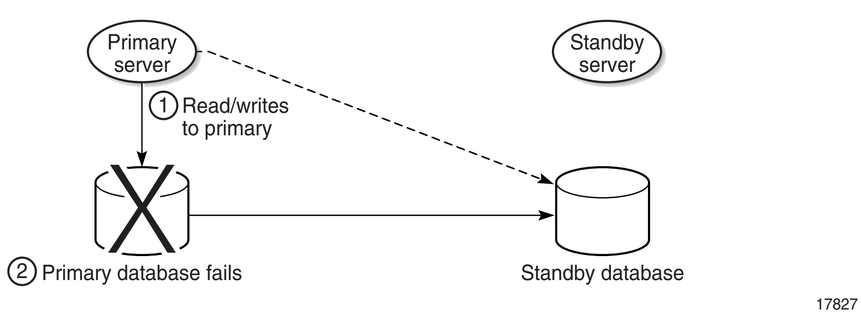
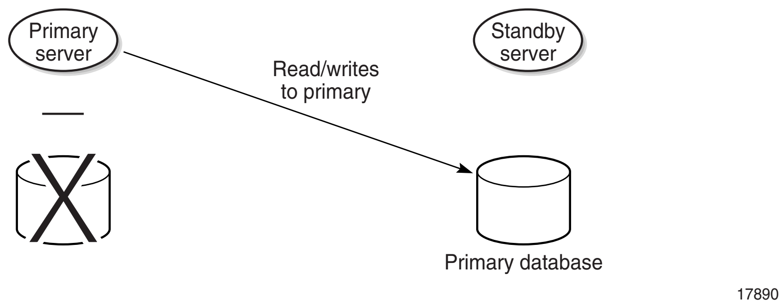


Figure 7-9 shows the server and database roles after a successful failover.

Figure 7-9 Server and database roles after database failover



Note — After a successful failover, database redundancy is not available. See "Re-establishing database redundancy" in this section for information about re-establishing database redundancy after a failover.

When a database failover fails, the primary server tries again to communicate with the primary database. If the primary database remains unavailable, the primary server tries again to initiate a failover.

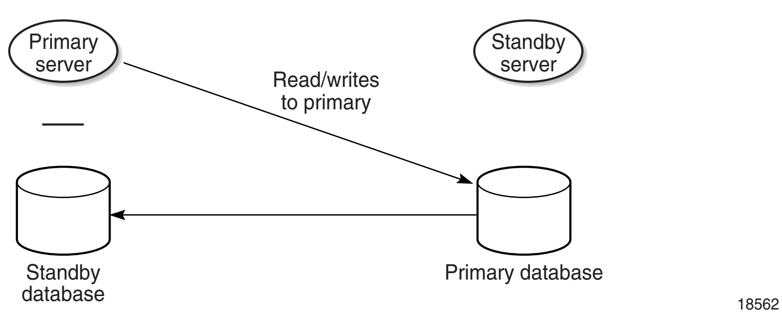
Re-establishing database redundancy

After a failover, the former primary database is no longer part of the redundant configuration. To re-establish database redundancy, you must reinstantiate the former primary database as the new standby database. You can do this only when the failed database station is restored to full operation and has a configured proxy port that is in service. See Procedures 7-6 and 7-7 for more information about manually reinstantiating a redundant database.

You can configure the 5620 SAM to automatically reinstantiate the former primary database as the new standby database. Automatic database reinstantiation occurs only in the event of a database failover. When the function is enabled, the 5620 SAM attempts an automatic reinstantiation every 60 minutes by default. You can enable automatic database reinstantiation during the 5620 SAM main server installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling and configuring automatic database reinstantiation.

Figure 7-10 shows a former primary database serving as the new standby database.

Figure 7-10 Server and database roles after database reinstantiation



Automatic database realignment

In a redundant 5620 SAM system that is geographically dispersed, the primary server and database may be in separate LANs or WANs after an activity switch or failover. The network latency that this introduces can affect 5620 SAM system performance. Automatic database realignment is an optional mechanism that attempts to ensure that each main server uses the local database.

The database with which a main server tries to align itself is called the preferred database of the main server. An operator enables automatic database realignment and specifies the preferred database during 5620 SAM server installation, or during server configuration after installation.

Note — For automatic database alignment to work, you must enable it and specify a preferred database on each main server in a redundant 5620 SAM system.

When a primary server starts, it verifies that the primary database is the preferred database. If the primary database is not the preferred database, the server performs a database switchover to reverse the primary and standby database roles. If the switchover is successful, the main servers and databases in the 5620 SAM system are aligned. If the switchover fails, each database reverts to the former role, and the main server raises an alarm about the failed switchover.

When you perform a database switchover and automatic database realignment is enabled, the primary server does not attempt database realignment. A switchover is a manual operation that is considered to be a purposeful act.

Performing a server activity switch when automatic database realignment is enabled triggers a database switchover.

Summary of redundancy operations

Table 7-1 summarizes the operations related to 5620 SAM main server redundancy.

Table 7-1 5620 SAM server redundancy operations

<table>
<tr><th>Type</th><th>Description</th><th>Notes</th></tr>
<tr><td>Server activity switch (automatic)</td><td>An automatic activity switch occurs when the primary server cannot communicate with the standby server.
An automatic server activity switch involves the following sequence of high-level events.
• The standby server cannot communicate with the primary server within 60 s, and the primary database cannot communicate with the primary server.
• The standby server performs an activity switch to become the new primary server. [(1)]
• If automatic database realignment is enabled, the new primary server attempts a database switchover.
• The new primary server establishes a connection to the primary database and begins to manage the network.
• The new primary server and the auxiliary servers synchronize the outstanding request information.</td><td rowspan="2">When the primary server detects a standby server communication failure, each GUI client receives notification of the failure.
During an activity switch, each client GUI displays a main server status message.
During an activity switch, a main server does not process SNMP traps from the network, and no NE resynchronizations occur. The auxiliary servers continue to process outstanding requests, and synchronize the request information with the new primary server after the activity switch.
When the communication failure is resolved, each GUI client receives notification that redundancy is restored.</td></tr>
<tr><td>Server activity switch (manual)</td><td>A manual activity switch is typically performed for maintenance or testing purposes during a scheduled maintenance period.
A manual server activity switch involves the following sequence of high-level events.
• The new primary server establishes a connection to the primary database and begins to manage the network.
• The new primary server and the auxiliary servers synchronize the outstanding request information.
• If automatic database realignment is enabled, the new primary server attempts a database switchover.
See Procedure 7-3 for information about performing a manual activity switch.</td></tr>
</table>

Note

(1) This activity switch is allowed only if the primary server does not retain control of the primary database.

Table 7-2 summarizes the operations related to 5620 SAM database redundancy.

Table 7-2 5620 SAM database redundancy operations

Type	Description	Notes
Database switchover	A database switchover is a manual operation that reverses the primary and standby database roles, for example, for primary database maintenance, or to realign database roles with database stations after a server activity switch. A switchover can occur only when the primary and standby databases are functioning correctly and can communicate with each other. A database switchover involves the following sequence of high-level events. • A 5620 SAM administrator initiates the switchover on a primary or standby server. • The main server asks each auxiliary server to release all database connections. The switchover fails if all database connections are not released within 15 minutes. • The main server directs the standby database to become the primary database. • The main server restarts to fully synchronize information with the new primary database. See Procedure 7-4 for information about performing a database switchover.	No automatic database realignment occurs after a database switchover.
Database failover	A database failover is an automatic reversal of the primary and standby database roles, for example, after a primary database failure. A database failover involves the following sequence of high-level events. • No main server can communicate with the primary database within a period that is 2 min by default. • The currently active main server directs the standby database to become the primary database. • If automatic database realignment is enabled and the primary server and database are not aligned, the primary server performs an activity switch. • The primary server directs each auxiliary server to connect to the new primary database.	When the primary server detects a communication failure with the primary or standby database, the GUI clients are informed that the database is not reachable. After the cause of the communication failure is resolved, the GUI clients are notified that the database is reachable. After a failover, you must reinstantiate the former primary database as the new standby database. Database redundancy is not restored until reinstantiation is complete. The 5620 SAM attempts to automatically reinstantiate the former primary database when automatic database reinstantiation is enabled.
Re-establishing database redundancy	Re-establishing database redundancy is a user action that uses database reinstantiation to restore the former primary database as the new standby database. After a failover, the former primary database is not available for redundancy until an operator or the 5620 SAM reinstantiates it as the new standby database. See Procedures 7-6 and 7-7 for information about re-establishing database redundancy after a failover.	The following conditions must be true before you can re-establish database redundancy. • The failover completes successfully. • The station that contains the primary database is operational. • The former primary database proxy port is configured and in service.

Redundancy scenarios

The following are redundancy failure scenarios and the 5620 SAM response to each:

- primary server cannot communicate with primary database—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If both the primary and standby servers cannot communicate to the primary database, the primary server initiates a database failover. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a server activity switch.
- primary server cannot communicate with managed NEs—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If automatic database realignment is enabled and the new primary server and the primary database are not aligned, the new primary server performs a database activity switch.
- primary server cannot communicate with primary database or managed NEs—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a database activity switch.
- primary server cannot communicate with primary database, managed NEs, or standby server—The standby server activates to become the new primary server. If automatic database realignment is enabled, the new primary server initiates a database activity switch.
- primary and standby servers cannot communicate with primary database—The primary server initiates a database failover. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a server activity switch.
- primary and standby servers cannot communicate with each other - primary server can communicate to primary database—The primary server continues to perform as a primary server and the primary database continues to perform as a primary database. An alarm will be raised to indicate the communication failure between primary server and standby server.
- primary and standby servers cannot communicate with each other - primary and standby servers can communicate to their respective preferred databases—The primary server continues to perform as a primary server and the primary database continues to perform as a primary database. The standby server will become the primary server and the standby database will become a primary database. There will be two separate primary servers and primary databases running in the network. An alarm will be raised to indicate the activity switch. The connected users will not get impacted as they continue their session with the original primary server. New users will continue to establish sessions with the original primary server. If a user explicitly tries to connect to a new primary server, the sessions will be established.

- primary and standby servers cannot communicate with each other—The primary server cannot communicate to its preferred database and the standby server cannot communicate with its preferred database.
- primary and standby server cannot communicate with the managed NEs—If both the primary server and standby server cannot communicate with the managed NEs but can communicate to the respective preferred databases, no server activity switch or database failover occurs. The NE status will be marked as not reachable and the appropriate reachability alarm will be raised.

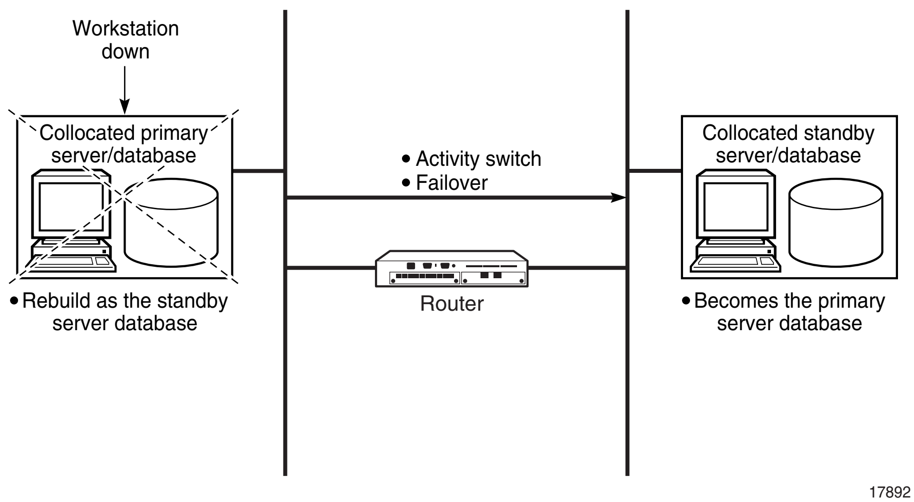
You can configure the following redundancy parameters to specify how a 5620 SAM system manages a loss of connection to the managed NEs:

- the number of elapsed seconds that constitute a loss of connectivity
- how often a main server refreshes the list of managed NEs
- the minimum number of NEs that must respond to a connectivity check

Contact your Alcatel-Lucent technical-support representative for more information.

Figure 7-11 shows the redundancy effect on a collocated configuration in which the station that hosts the primary server and database becomes unresponsive.

Figure 7-11 Primary database and server station down, collocated system

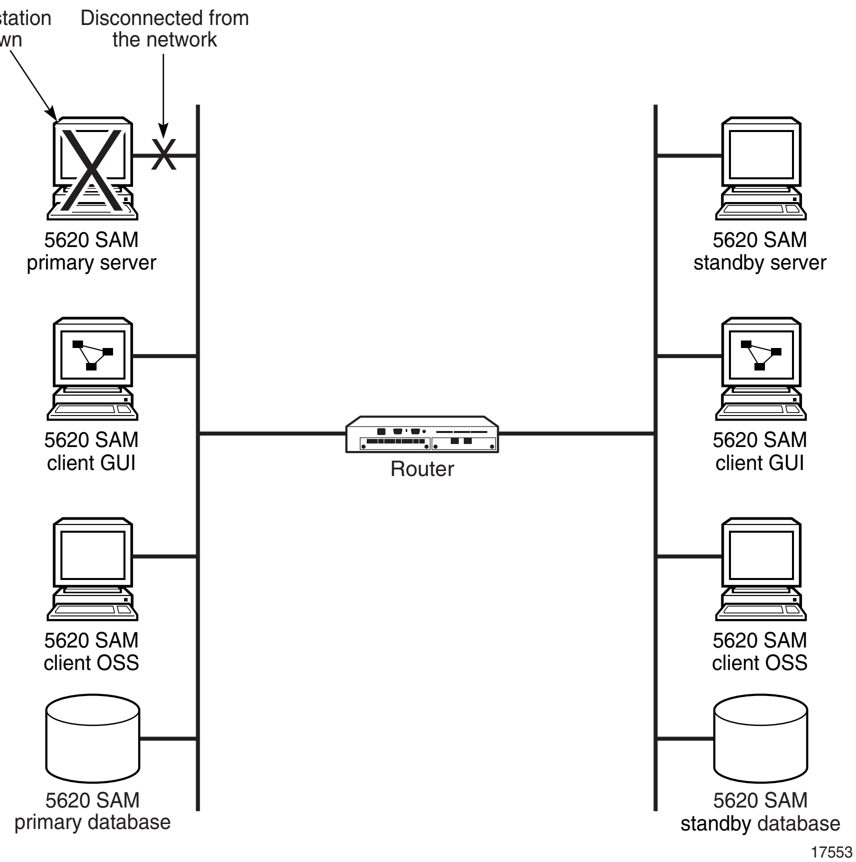


The following occurs when the primary station becomes unresponsive:

- The standby server and database become the primary server and database.
- Redundancy is not restored until the former primary station is rebuilt as the new standby station.

Figure 7-12 shows a primary server disconnection from the network in a distributed 5620 SAM system.

Figure 7-12 Primary server disconnected from network, distributed system

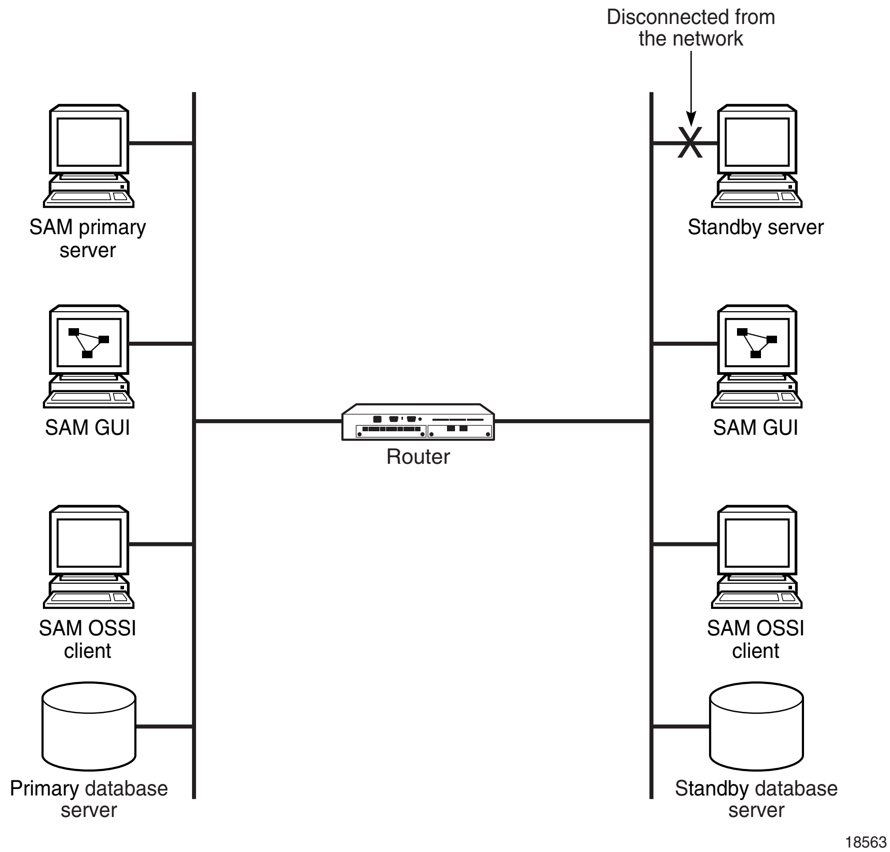


The following occurs when the primary server is disconnected from the management network:

- The standby server detects the loss of connectivity with the primary server and becomes the new primary server.
- The new primary server raises alarms about the unavailability of the former standby server and the activity switch.
- If automatic database realignment is enabled, the new primary server performs a database switchover.
- When connectivity is restored, the former primary server reconnects to the network as the new standby server.

Figure 7-13 shows a standby server disconnection from the network in a distributed 5620 SAM system.

Figure 7-13 Standby server disconnected from network, distributed system



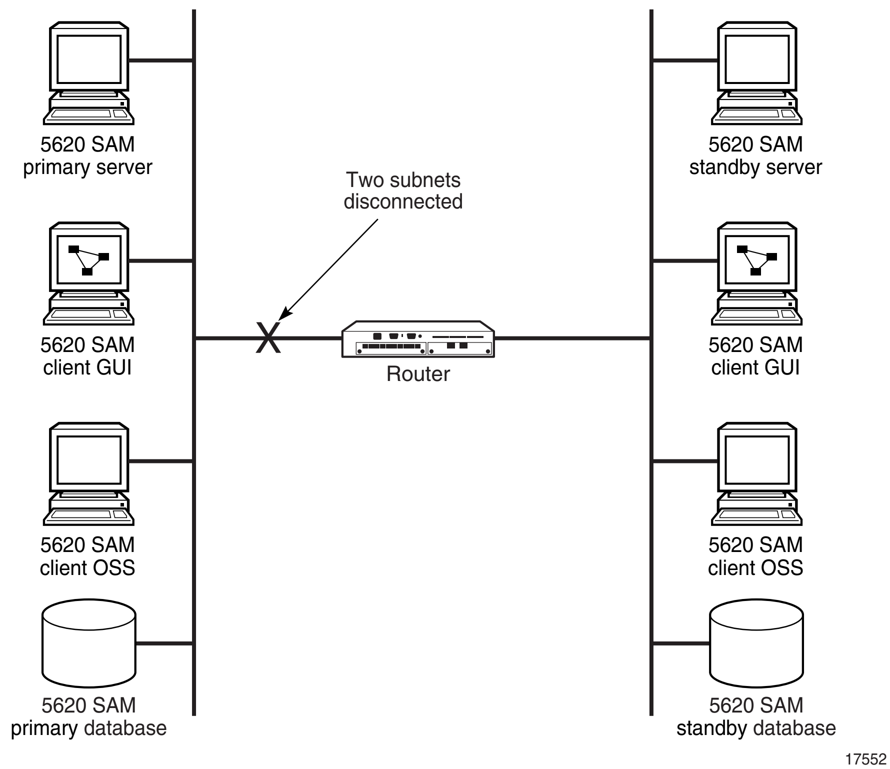
The following occurs when the standby server is disconnected from the network:

- The standby server tries to become the primary server because it cannot contact the primary server, so assumes that it is down.
- The primary server raises an alarm to indicate that the standby server is down.

After the standby server reconnects to the network, it resumes the role of standby server and the standby down alarm is cleared.

Figure 7-14 shows a network failure in a distributed 5620 SAM system.

Figure 7-14 Network failure, distributed system



The following occurs when the primary and standby servers are in separate subnets and cannot communicate:

- The original primary server raises an alarm about the standby server unavailability, and each GUI client displays the standby server status as Down.
- The standby server becomes a primary server. The original primary server continues to operate as a primary server.

Note — You can eliminate a single point of hardware or network failure by using redundant interfaces and redundant physical network paths. See the *5620 SAM Planning Guide* for more information.

7.2 Workflow for configuring 5620 SAM system redundancy

1 Configure redundancy during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

2 As required, perform manual activity switches and switchovers.

a For 5620 SAM main servers:

i Verify the redundancy status of the 5620 SAM software. See Procedure 7-1 for more information.

ii Perform a manual activity switch on the primary server. See Procedure 7-3 for more information.

iii Validate the updated redundancy status. See Procedure 7-1 for more information.

b For 5620 SAM databases:

i Verify the redundancy status of the 5620 SAM software. See Procedure 7-1 for more information.

ii As required, perform a switchover. See Procedures 7-4 and 7-5 for more information.

iii As required, configure automatic database realignment. See Procedure 7-8 for more information.

iv Validate the updated redundancy status. See Procedure 7-1 for more information.

3 After a failover, re-establish redundancy between the standby and primary databases. See Procedures 7-6 and 7-7 for more information.

7.3 5620 SAM system redundancy procedures

Use the following procedures to perform redundancy tasks.

Procedure 7-1 To view the 5620 SAM main server and database status

1 View the Standby Server and Standby DB status indicators in the 5620 SAM client GUI task bar. Each indicator should display Up.

2 Choose Administration→System Information. The System Information form opens with the General tab displayed.

3 View the general redundancy information:

- Domain Name—the 5620 SAM domain name specified at installation
- Redundancy Enabled—selected if redundancy is enabled
- Alignment Enabled—selected if automatic database realignment is enabled; displayed only if the 5620 SAM system is redundant
- Realignment Status—Aligned or Not Aligned

4 View the following information in the Primary Server panel:

- Host Name—the host name of the primary or standalone main server
- Status—Unknown, Down, or Up

5 View the following information in the Primary Database Server panel:

- Instance Name—the name of the primary database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the primary database
- Host Name—the host name of the primary database, or of the database in a standalone 5620 SAM system

6 If the 5620 SAM system is redundant, view the following information in the Standby Server panel:

- Host Name—the host name of the standby main server
- Status—Unknown, Down, or Up

7 If the 5620 SAM system is redundant, view the following information in the Standby Database Server panel:

- Instance Name—the name of the standby database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the standby database
- Host Name—the host name of the standby database

8 Click on the Properties button to display additional information about the primary or standalone 5620 SAM main server. The Main Server properties form opens.

9 View the following general main-server information:

- Host Name—the host name of the primary main server
- Server Type—Main
- Resource Managed—selected if the main server is included in 5620 SAM resource management

10 View the following information in the Client Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the 5620 SAM GUI and OSS clients through a NAT router
- Public IP Address—the IP address that the 5620 SAM GUI and OSS clients use to reach the main server through a NAT router

Note 1 — The Private IP Address and Public IP Address display 0.0.0.0 when the 5620 SAM clients and the main server use host names, rather than IP addresses, for communication.

Note 2 — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and clients.

11 View the following information in the Redundant Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the standby main server through a NAT router
- Public IP Address—the IP address that the standby main server uses to reach the primary main server through a NAT router
- Peer Public IP Address—the IP address that the standby main server uses to reach the main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the primary and standby main servers.

12 View the following information in the Auxiliary Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the auxiliary servers through a NAT router
- Public IP Address—the IP address that the auxiliary servers use to reach the primary main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and the auxiliary servers.

13 Close the Main Server properties form. The System Information form reappears.

14 Click on the Database button to view more detailed database information, if required. See chapter 8 for information about the 5620 SAM database.

15 Click on the Faults tab to view alarm information, if required.

16 Close the System Information form.

Procedure 7-2 To view the 5620 SAM auxiliary server status

1 Choose Administration→System Information. The System Information form opens.

2 Click on the Auxiliary Servers tab button.

3 Review the list of auxiliary servers.

4 Select an auxiliary server in the list and click on the Properties button. The properties form for the auxiliary server opens.

5 Review the auxiliary server information, which includes the following:

- Host Name—the host name of the auxiliary server
- Port Number—identifies the port that the auxiliary server uses to communicate with each main server and database
- Auxiliary Server Type—Reserved or Preferred
- Server Status—Unknown, Down, Up or Unused
- Resource Managed—selected if the auxiliary server is included in 5620 SAM resource management
- Public IP address—the IP address that the main servers use to reach the auxiliary server

6 Perform one of the following:

a View the following main server information for a redundant 5620 SAM system:

- Server 1 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
- Server 2 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server

b View the following main server information for a standalone 5620 SAM system:

- Server Public IP address—the IP address that the auxiliary server uses to communicate with the main server

7 Click on the Auxiliary Services tab button.

8 Review the list of auxiliary services.

9 Review the information for each auxiliary service, which includes the following:

- Service Name—the type of service, for example, statistics collection
- Selected—indicates whether this auxiliary server is currently used by a main server to process requests
- IP Address—the IP address that each main server uses to reach the auxiliary server
- Host Name—the host name of this auxiliary server
- Auxiliary Server Type—Reserved or Preferred

10 Close the Auxiliary Services form.

11 Click on the Faults tab to view alarm information, if required.

12 Close the System Information form.

Procedure 7-3 To perform a server activity switch

Perform this procedure to reverse the primary and standby roles of the main servers in a redundant 5620 SAM system. Consider the following before you perform a server activity switch.

- Each client GUI receives notification of a server activity switch.
- During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics.
- During a server activity switch, auxiliary servers process outstanding requests, but do not communicate with a main server.
- After a server activity switch, the new primary main server deploys outstanding configuration changes to NEs, establishes communication with the auxiliary servers, and synchronizes information with the auxiliary servers.
- A manual activity switch stops and starts the former primary main server. Server redundancy is unavailable until the former primary main server is fully initialized as the new standby main server.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

bash$ ***install_dir*/nms/bin/nmsserver.bash force_restart** ↵

where *install_dir* is the 5620 SAM server installation location, typically /opt/5620sam/server

The server activity switch begins. The primary main server restarts as the standby main server, and the former standby main server becomes the new primary main server.

4 Close the console window.

5 Clear alarms, as required. The activity switch alarms must be cleared manually.

6 Verify that the GUI and OSS clients can connect to the new primary main server.

Procedure 7-4 To perform a 5620 SAM database switchover using the 5620 SAM client GUI

Perform this procedure to use the 5620 SAM client GUI to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

1 Log in to the client GUI as a 5620 SAM user with the admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Click on the More Actions button and choose Switchover. A dialog box appears.

Note — The Switchover option is disabled when the proper switchover conditions are not in place, for example, when a switchover or failover is in progress.

4 Respond to the dialog-box prompt.

5 Click on the Yes button. The 5620 SAM server performs the database switchover.

6 Close the System Information form.

Procedure 7-5 To perform a 5620 SAM database switchover using a CLI script

Perform this procedure to use a CLI script to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

```
bash$ install_dir/switchoverdb.bash username password ↵
```

where

install_dir is the 5620 SAM server installation location, typically /opt/5620sam/server

username and *password* are the login credentials for a 5620 SAM client account that has the required privilege level and scope of command

The script displays the following confirmation message:

```
The standby database will become the new primary database,

and the old primary will become the new standby.

Do you want to proceed? (YES/no) :
```

4 Enter the following case-sensitive text at the prompt to start the switchover:

YES ↵

The 5620 SAM server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

5 Close the console window when the database switchover is complete.

Procedure 7-6 To reinstantiate a redundant database using the 5620 SAM client GUI

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database.

When automatic database reinstantiation is enabled, a failed manual reinstantiation attempt does not affect the reinstantiation timer. In the case of a successful manual reinstantiation, further reinstantiations are not attempted by the 5620 SAM.

Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

1 Log in to the client GUI as a user with the 5620 SAM admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Verify the database redundancy status matches the following:

- Failover State: Successful
- Switchover State: Not Attempted

4 Click on the More Actions button and choose Re-Instantiate Standby. A dialog box appears.

5 Click on the Yes button to confirm. The database reinstantiation begins.

The client GUI status bar and the System Information form display the reinstantiation status. The Standby Re-instantiation State changes from In Progress to Success when reinstantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current reinstantiation.

6 Close the System Information form when the reinstantiation is complete.

Procedure 7-7 To reinstantiate a redundant database using a CLI script

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database. Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following at the CLI prompt:

bash$ **./reinstantiatedb.bash -u *username* -p *password*** ↵

where

username is the user name of a 5620 SAM client account that has the required privilege level and scope of command

password is the password for the user account

The script displays the following confirmation message:

```
This action will rebuild the standby database.

Do you want to proceed? (YES/no) :
```

5 Enter the following case-sensitive text at the prompt to begin reinstantiation:

YES ↵

The 5620 SAM server begins to reinstantiate the former primary database as the standby database. Progress is indicated by a rolling display of dots in the console window. Database reinstantiation is complete when the CLI prompt reappears.

6 Close the console window when the reinstantiation is complete.

Procedure 7-8 To configure automatic database realignment

Perform this procedure to enable or disable automatic database realignment on the main servers.

Caution — This procedure requires a restart of a 5620 SAM main server, which is service-affecting. To avoid service interruption, schedule the reconfiguration to coincide with a maintenance window.

Note 1 — This procedure applies only to redundant 5620 SAM deployments.

Note 2 — You must perform this procedure first on the standby main server station, and then on the primary main server station.

1 Log in to the standby main server as the samadmin user.

2 Stop the main server software.

i Navigate to the server binary directory. Enter the following at the prompt:

bash$ **cd *install_dir*/nms/bin** ↵

where *install_dir* is the server installation location, typically /opt/5620sam/server

ii Enter the following at the prompt:

bash$ **./nmsserver.bash stop** ↵

iii Enter the following at the prompt:

bash **./nmsserver.bash appserver_status** ↵

iv The server application is stopped when the command in step 2 iii returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 2 iii. Do not proceed unless the console displays the above text.

3 Enter the following to switch to the root user:

bash$ **su -** ↵

4 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

5 Navigate to the DVD_ROM drive.

6 Perform one of the following to open the 5620 SAM server installer.

a On a SPARC station:

i Enter the following:

cd Solaris ↵

ii Enter the following:

./ServerInstall_SAM_9_0_*revision*.bin ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

b On an x86-based station:

i Enter the following:

cd Solarisx86 ↵

ii Enter the following:

./ServerInstall_x86_SAM_9_0_*revision*.bin ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

7 Click on the Next button.

8 Accept the terms of the license agreement in the “Software License Agreement” panel.

9 Click on the Next button.

10 Choose Main Server Configuration in the “Choose Installation Type” panel.

11 Click on the Next button.

12 Click on the Next button in each subsequent panel until the “Database Alignment” panel is displayed.

13 Configure the “Enable Database Alignment” parameter.

Note — You must configure this parameter the same way on the standby and primary main servers.

14 If you selected the “Enable Database Alignment” parameter in step 13, select a server to act as the preferred server.

15 Click on the Next button.

16 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

17 Select the “Start the 5620 SAM Main Server” parameter.

18 Click on the Done button to close the server configuration utility.

19 Enter the following to switch back to the samadmin user:

```
# exit ↵
```

20 Verify the standby main server has started.

21 Log out of the standby main server.

22 Perform steps 1 to 21 on the primary main server.

Note — When you stop the primary main server, a switchover to the standby main server will occur.

23 If required, perform Procedure 7-3 to perform a server activity switch and revert the main servers to their original roles.

8 — 5620 SAM database management

8.1 5620 SAM database management overview

You can use the 5620 SAM database manager to do the following:

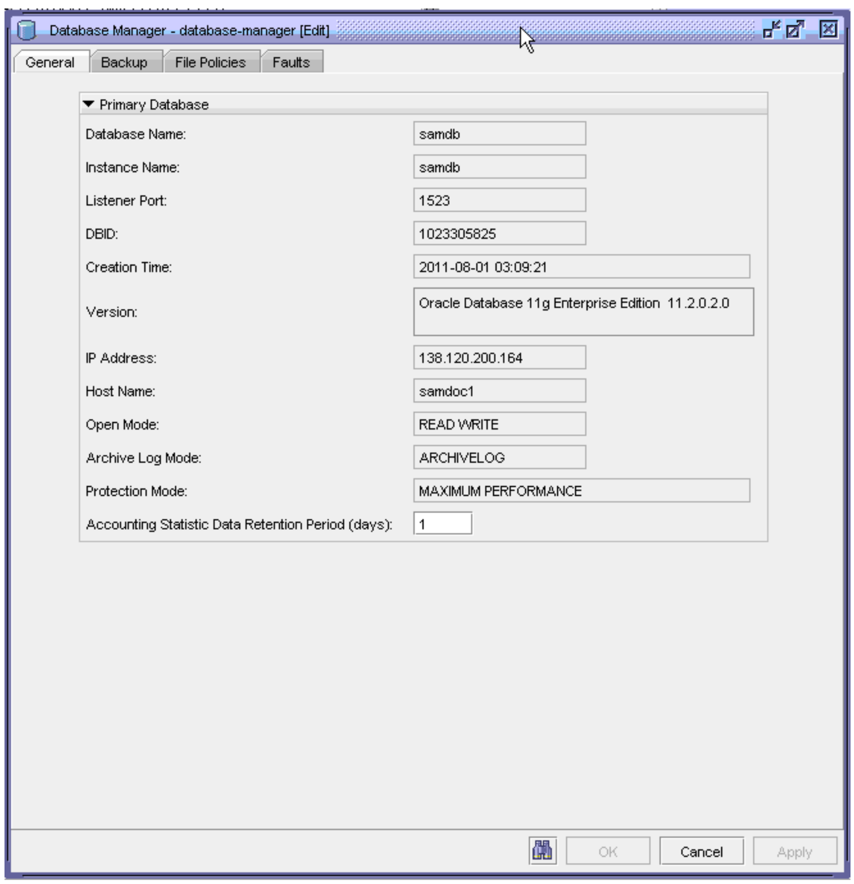
- view database parameters
- configure database parameters
- manage database log storage
- back up a database
- restore a database
- troubleshoot a database

Note 1 — The station to which you restore a 5620 SAM database must have the same OS as the station from which the backup is obtained, for example, Solaris SPARC, or the restore fails.

Note 2 — The 5620 SAM backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.

Figure 8-1 shows the General tab of the Database Manager form.

Figure 8-1 Database Manager form — General tab



See the *5620 SAM Maintenance Guide* for information about restoring a 5620 SAM database.

8.2 Workflow to manage the 5620 SAM database

1. Discover the network devices. The database of the managed devices is stored in the 5620 SAM database. See chapter 14 for more information.
2. Configure data retention parameters according to company policy. See Procedure 8-1 for more information.
3. Perform regular database management according to company policy.
   - i Monitor the database as required. See Procedure 8-2 for more information.
   - ii Back up the database as required. Alcatel-Lucent recommends that you back up the database daily. See Procedures 8-3 and 8-4 for more information.
   - iii Manage disk space by configuring policies to limit the maximum size of database log files, such as the alert, trace, listener, and audit logs. See Procedure 8-5 for more information.

8.3 5620 SAM database procedures

Use the following procedures to perform database management tasks.

Procedure 8-1 To configure statistics data retention for the 5620 SAM database

1. Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.
2. Configure the Accounting Statistic Data Retention Period (Days) parameter.

   Caution — Configuring the Accounting Statistic Data Retention Period (Days) parameter can affect 5620 SAM system performance. Consult an Alcatel-Lucent support representative before you configure the parameter.

3. Click on the OK button. A dialog box appears.
4. Click on the Yes button.
5. Close the Database Manager (Edit) form.

Procedure 8-2 To view the database properties

Perform this procedure to view general information about the Oracle database that the 5620 SAM uses.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens and displays information that includes the following:

- Database Name—created during 5620 SAM installation; the default is samdb
- Instance Name—created during 5620 SAM installation; the default is samdb
- Listener Port—the port on the server used for database communication
- DBID—the Oracle database ID, sometimes referred to as the SID
- Creation Time—the database creation time
- Version—the Oracle version identifier, for example, Oracle Database 11g Enterprise Edition 11.2.0.2.0
- IP Address—the IP address that the server uses as the destination address for communicating with the database
- Host Name—the host name of the database station
- Open Mode—specifies the type of database access, either READ or READ WRITE
- Archive Log Mode—specifies whether to archive the database log files; this is configured during database installation
- Protection Mode—the database protection mode, which is set by default during installation to MAXIMUM PERFORMANCE

2 View the information.

3 Close the Database Manager (Edit) form.

Procedure 8-3 To back up the 5620 SAM database using the client GUI

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one station to another
- To recover from hardware or software errors

- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 The database must be in ARCHIVELOG mode to perform a backup. Perform Procedure 8-2 and ensure that Archive Log Mode is set to ARCHIVELOG.

2 Click on the Backup tab button.

3 Perform one of the following.

a Configure a scheduled full or partial database backup. A full backup backs up the entire 5620 SAM database whereas a partial backup contains no accounting statistics data.

i Configure the parameters.

Note — Ensure that the Scheduled Backup Directory location is not tampered with and has more than enough space to contain the number of database backups specified by the Number to Keep parameter.

ii Select the Schedule Enabled parameter.

b Perform an unscheduled full database backup. A full backup backs up the entire 5620 SAM database.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup

ii Click on the Full Backup button. A dialog box appears.

iii Click on the Yes button. The full backup starts. The Backup State shown on the form changes to In Progress.

c Perform an unscheduled partial database backup. A partial backup contains no accounting statistics data.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup ii Click on the Partial Backup button. A dialog box appears.

iii Click on the Yes button. The partial backup starts. The Backup State shown on the form changes to In Progress.

4 Configure the Enable Backup File Compression parameter.

5 View the information in the Backup Status panel, if required. This information includes the following:

- Scheduled Backup—whether a backup schedule is configured
- Backup State—the state of the current or previous backup operation; the Backup State is dynamically updated during a backup operation
- Next Scheduled Backup Time—the next scheduled backup time
- Last Successful Backup Time—when the previous successful backup completed
- Last Successful Backup Type—the type of previous successful backup completed
- Last Attempted Backup Time—when the previous attempted backup took place
- Last Attempted Backup Type—the type of backup that was last attempted
- Directory of the Last Successful Backup—the storage location of the previous successful backup

6 Close the Database Manager (Edit) form.

Note — After backing up and restoring a database, you must perform a full resynchronization of the network to discover the recent managed device information changes.

Procedure 8-4 To back up the database using a CLI script

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one station to another
- To recover from hardware or software errors

- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 Log in as the Oracle management user on the database station. In a redundant 5620 SAM system, this is the station that holds the primary database.

2 Open a console window.

3 Enter the following at the console prompt to begin the database backup:

path*/install/config/samdb/SAMbackup.sh *backup_directory ↵

where
path is the 5620 SAM database installation location, typically /opt/5620sam/samdb
backup_directory is the directory that is to contain the database backup

Caution — When you back up a 5620 SAM database, you must specify a backup directory path that does not include the 5620 SAM database installation directory, or data loss may occur. The typical 5620 SAM database installation location is /opt/5620sam/samdb.

The database backup begins. A database backup can take several hours to complete.

4 Close the console window when the database backup is complete.

Procedure 8-5 To manage alert, listener, trace, and audit database log files

You can use policies to manage the file size of stored alert, trace, listener, and audit log files. When the size and number of files are left unbounded, exceeding database disk space limits may become a problem. The default settings of the file policies reduce the number of log files that are kept.

Database log files are compressed and stored in the alert log directory (for trace, alert, and audit log files) or the listener directory for listener log files.

For historical or troubleshooting purposes, Alcatel-Lucent recommends that you archive the database log files.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 Click on the File Policies tab button.

3 Perform one of the following.

a Create a new database file policy.

i Click on the Database File Policies button. The Database File Policies form opens.

ii Click on the Create button. The File Policy (Create) form opens.

iii Configure the parameters:

- ID
- Description
- Auto-Assign ID
- Purge Mode
- Max (Collective) Log Size
- Number of Archives

iv Click on the OK button. The File Policy (Create) form closes.

v Close the Database File Policies form.

b Modify an existing policy.

i Click on the Database File Policies button. The Database File Policies form opens.

ii If required, specify a filter and click on the Search button.

iii Select a policy from the list and click on the Properties button. The File Policy (Edit) form opens.

iv Configure the parameters:

- Description
- Purge Mode
- Max (Collective) Log Size
- Number of Archives

v Click on the OK button. The File Policy (Edit) form closes.

vi Close the Database File Policies form.

4 Associate the file policy with a database log type, if required.

i Click on the Select button beside one of the following:

- Alert Log File Policy
- Listener Logs File Policy
- Trace and Audit Logs File Policy

The Database File Policies - Database Manager (Edit) form opens.

ii Choose a policy from the list.

iii Click on the OK button. The Database File Policies - Database Manager (Edit) form closes and the policy identifier is displayed on the Database Manager (Edit) form.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Database Manager (Edit) form closes.

9 — 5620 SAM user security

9.1 5620 SAM user security overview

A 5620 SAM client GUI operator can use security management forms to configure and manage the following:

- 5620 SAM users and user groups, which are assigned the following configurable profiles:
    - scope of command profiles, which define the level of user control over objects in scope of command roles
    - span of control profiles, which define the 5620 SAM objects that users can view and manage
- 5620 SAM user-account and password expiry periods
- GUI inactivity timeout periods
- password history counts
- the number of active and allowed client sessions
- the GUI login form, which can display a customized login message
- user activity logs, which record the actions performed by each user

User accounts and user groups

You can use 5620 SAM user accounts and user groups to do the following:

- Provide GUI or OSS access to the 5620 SAM functional areas that match specific operator requirements.
- Restrict access to functions or objects based on operator expertise or authority.

Users have view access, read-write access, or no access to 5620 SAM objects and functions based on the following:

- the user group to which they belong
- the scope of command profile assigned to the user group.

The 5620 SAM user account called admin is created during 5620 SAM installation. The admin account is assigned the administrator scope of command role and a span of control profile that has Edit Access assigned to each default span. See “Scope of command” in this section for more information.

Caution — Because the 5620 SAM is unable to obtain an authentication secret value from an NE, Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret on an NE. If you configure a shared authentication secret on a managed NE using another interface, for example, a CLI, the 5620 SAM cannot synchronize the security policy with the NE.

Note — To restrict user access to top-level 5620 SAM functions such as 5620 SAM and NE security management, Alcatel-Lucent recommends the following:

- Assign the administrator scope of command role to a minimal number of 5620 SAM user accounts.
- Assign each 5620 SAM user to a user group that has the minimum privileges for performing the required tasks.

Only the admin user, or a user whose scope of command includes write access to the security package, can perform the tasks listed in Table 9-1.

Table 9-1 5620 SAM security-related tasks

Task:	See:
Create a proprietary user login statement	Procedure 9-1
Specify expiry periods for user accounts, passwords, and GUI inactivity checks	Procedure 9-3
Specify responses to authentication failures	Procedure 9-5
Create or modify scope of command roles	Procedure 9-8
Create or modify scope of command profiles	Procedure 9-9
Create or modify span of control profiles	Procedure 9-13
Assign 5620 SAM objects to a span	Procedure 9-12
Create or modify user groups	Procedure 9-17
Create users and assign users to user groups	Procedure 9-18
Specify a default external user group	Procedure 9-23
Search for inactive user accounts	Procedure 9-24
Suspend and reinstate users	Procedure 9-25
Modify user passwords	Procedure 9-26
Send text messages and notifications to some or all GUI clients	Procedure 9-31
Shut down GUI or 5620 SAM-O JMS client sessions on a per-client basis	Procedure 9-32
View user logs	Procedure 9-33
Enable LI management	Chapter 34

The following general rules apply to 5620 SAM users and user groups:

- Only database space limits the number of users and user groups that can be created.
- A user cannot belong to more than one user group.
- Only one session per user account can be open at the same time on a client station.
- A scope of command profile allows user-group access to one or more 5620 SAM functional areas.
- A span of control profile allows user-group access to one or more 5620 SAM managed objects.

- A user group is associated with only one scope of command profile that can contain multiple scope of command roles.
- A user group is associated with only one span of control profile that can contain multiple spans.
- The assigned user privileges determine the following for a GUI user:
    - the available 5620 SAM menu options
    - the parameters on object property forms that are configurable
- By default, each user group is assigned access to all 5620 SAM objects.
- A user inherits span of control access rights from their assigned user group.
- When you modify a user group, and a user in the group has an open client session, client operations may fail for the user. To put the new user group permissions into effect, the user must close the current client session and open a new session.
- You can modify, but not delete, a span of control profile that is assigned to a user group.

Password management

A 5620 SAM user password must observe the following constraints:

- be 8 to 100 characters long
- contain at least three of the following character types:
    - lowercase
    - uppercase
    - special
    - numeric
- not be the user account name in forward or reverse order
- not contain more than three consecutive instances of the same character
- be changed according to a configurable schedule to prevent account lockout
- not be reused as a new password for the same user account

Scope of command

The scope of command for a user defines what the user is allowed to do; it is a collection of one or more configurable roles, or sets of permissions. A scope of command profile that contains one or more roles, and the profile is subsequently applied to a user group. Each user in the group inherits the access rights specified in the scope of command profile.

Roles

A scope of command role specifies the read, create, update, and delete access permissions for a 5620 SAM object type or package. You can create custom roles by assigning specific access permissions to different 5620 SAM functional areas. These functional areas are organized in packages, methods, and classes. See Appendix A for a listing of all access permissions that can be assigned to a scope of command role.

Note 1 — When you enable the Create permission on a 5620 SAM package, method, or class, the Update permission is automatically enabled.

Note 2 — When you enable the Update permission on a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

You can create an original scope of command role, or copy an existing role and modify the role permissions to create a new role. The 5620 SAM has several predefined scope of command roles. See Appendix A for a listing of the permissions, access levels, and descriptions of all predefined scope of command roles and profiles.

Note — When you create a scope of command role, you must enable create, update/execute, and delete access to allow the modification of a class or package.

Profiles

A scope of command profile contains one or more scope of command roles, and is assigned to a user group. Each user in the group inherits the permissions from the scope of command roles in the profile.

Span of control

The span of control for a user is a list of the objects over which the user has control, for example, a grouping of NEs or services. You can create an original span, or copy an existing span and modify the list of associated objects to create a new span. The objects that are in a span, or that can be added to a span, are called span objects.

The 5620 SAM has several predefined spans. Each new 5620 SAM object, for example, a discovered NE, is added to the corresponding predefined span. Table 9-2 lists the predefined 5620 SAM spans and the type of span objects in each.

Note — You cannot modify or delete a predefined span.

Table 9-2 Predefined 5620 SAM spans

Span	Included objects
Default Topology Group Span	Topology groups
Default Router Span	Managed NEs
Default Script Span	CLI and XML API scripts, service templates, tunnel templates, and auto-provision profiles
Default Test Suite Span	Test suites
Default Group Span	Ring groups and VLAN groups
Default Bulk Operation Span	Bulk operations
Default Service Span	Services
Default Customer Span	Customers
Default Transport Span	Optical wavelength services

Spans are specified in span of control profiles that are associated with user groups. A user can create a new 5620 SAM object only when the predefined span for the object type is in the span of control profile. For example, if you do not have the Default Group Span in your span of control profile, you cannot create a ring group.

NEs are added implicitly to a span when the parent topology group, ring group, or VLAN group is in a span. An object that is implicitly added to a span cannot be removed from the span, but an explicitly added object can be removed.

Note 1 — A user can view or configure a point-to-point connection only when each endpoint of the connection is in the user span of control. For example, if the endpoints of an LSP path are in different spans, you must have view or configuration privileges in each span in order to view or configure the LSP path.

Note 2 — During span modification, you can drag and drop NEs and topology groups into the span contents list.

Each user can control which objects the 5620 SAM displays in maps, lists, and navigation trees, based on the user span of control. The User Preferences form contains a parameter that globally specifies whether the Edit Access span objects of the user are shown by default. Objects that are not in a View Access span of the user are never displayed, regardless of the user preference. See chapter 3 for information about configuring the user span of control display preference.

In a list form, a user can override the global display preference using the Span On parameter. When the form is a filtered list form, such as a topology map, the Manage Services form or the Alarm Window, the associated advanced filter form contains a selector for filtering the search results based on the span of control. See chapter 3 for information about configuring span of control filters.

Profiles

A span of control profile is a collection of one or more spans that is assigned to a user group. Each span in a profile is assigned one of the following access designations during profile creation:

- View Access—The user can view the span objects, unless the scope of command permissions deny read access.
- Edit Access—The user can view and modify the span objects, unless the scope of command permissions deny access.
- Blocked Edit—The user can view but not modify the span objects, regardless of the scope of command permissions.
- Blocked View—The user cannot view or modify the span objects, regardless of the scope of command permissions.

Blocked Edit and Blocked View spans restrict access to a subset of the objects in another span in the same profile. For example, if multiple span of control profiles each contain the Default Service Span, you can add a customer-specific Blocked View or Blocked Edit span to each profile so that the user group associated with a profile can view or configure only the services of specific customers.

A Blocked Edit or Blocked View span takes precedence over other spans. For example, if a user has an Edit Access span that contains all services and a Blocked View span that contains Customer A and Customer B, the user cannot view or configure the services that belong to Customer A and Customer B.

Caution — Alcatel-Lucent recommends that you carefully plan and consider the effects of combining customer, service, and NE spans in a span of control profile. For example, a user can modify a service only when the service, customer, and participating NEs are in one or more Edit Access spans of the user, and none of these objects is in a Blocked Edit or Blocked View span.

To ensure that span conflicts do not interfere with network troubleshooting, the 5620 SAM allows a user to execute tests on NEs and service sites that are not in an Edit Access span of the user. However, activities such as policy distribution, software upgrades, and statistics collection can be performed only by a user with Edit Access spans that contain the target objects.

When you upgrade the 5620 SAM from a release earlier than 8.0 to Release 8.0 or later, the 5620 SAM automatically assigns all of the predefined spans to each existing span of control profile. The Default Customer and Default Service spans are assigned as Edit Access spans to preserve the existing user privileges; each of the other spans is assigned as a View Access span.

Span rules

By default, the 5620 SAM automatically adds a new service to the Default Service span. Using an OSS or GUI client, you can create policies called span rules that direct the 5620 SAM to add new services to other spans in addition to the Default Service span.

A span rule is associated with a format or range policy, and applies to the users and user groups named in the format or range policy. You can associate multiple range policies with one user and service type. This enables the automatic addition of a new service to a specific span based on the Service ID chosen during service creation.

During span rule creation, you must specify one of the following to indicate which spans receive the services that the user creates:

- the Edit Access spans of each user associated with the format or range policy
- each span that is explicitly named in the rule

The span rules associated with a format or range policy take effect for new services only if the format or range policy is administratively enabled and has a valid configuration that includes at least one user or user group.

See “Sample span rule configuration” in this chapter for a sample span rule configuration and implementation.

Remote authentication and authorization for users with no 5620 SAM user account

The 5620 SAM uses a JAAS security framework to provide authentication and authorization services. When a user logs in to the 5620 SAM, the authentication method used depends on the 5620 SAM login module configuration. The 5620 SAM supports the following remote authentication login modules:

- RadiusJaasLoginModule
- TacacsPlusJaasLoginModule

The JAAS security framework integrates the login modules with the 5620 SAM. During startup, the 5620 SAM reads a file that contains the JAAS login module configuration. Depending on the VSA configuration in the file, one of the following authentication and authorization methods is available for remote users that do not have a 5620 SAM user account:

- The remote server authenticates the user and the 5620 SAM assigns a user group.
- The remote server authenticates the user and assigns a user group.

When the 5620 SAM assigns a user group to a remote user, a default external user group must be present in the 5620 SAM. User authentication succeeds when the remote authentication server validates the user password. User authorization succeeds and the user is provided with access rights when the default external user group is associated with the user. The 5620 SAM then creates a remote user account for the login session. In this scenario, when the default external user group is not specified, authorization fails and the user is denied access.

When the remote authentication server assigns a user group to a remote user, VSA support must be enabled in the JAAS login module configuration. In this scenario, a user group must be defined on the remote authentication server, and the remote server administrator must load the 5620 SAM RADIUS dictionary on the RADIUS server. The Sam-security-group-name VSA in the dictionary is used to configure a RADIUS remote user on the RADIUS server. The user group that is defined in the VSA must exist in the 5620 SAM. The remote authentication server administrator must specify the user group in the user configuration on the authentication server.

When the remote user logs in to the 5620 SAM, authentication succeeds when the remote authentication server validates the user password. Authorization succeeds and the user is provided with access rights when the user group defined on the remote server is sent to the 5620 SAM and validated. If the user group name matches a user group name in the 5620 SAM, the 5620 SAM creates a remote user account for the login session. Otherwise, authorization fails and user access is not granted.

See Procedure 9-23 for information about how to configure remote authentication and authorization for remote-only users.

In RADIUS, the authentication success message that is sent to the 5620 SAM contains the user group name. In TACACS+, authentication must succeed before an authorization message containing the user group name is sent to the 5620 SAM.

Successful remote authentication for an OSS user requires that the remote server and the 5620 SAM use the same password format. The OSS users can log in using a clear text password or an MD5 hashed password if the remote authentication server supports MD5 password hashing. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

When a remote 5620 SAM GUI or OSS session terminates, the user account for the session does not get deleted. This allows remote authenticated users to keep details such as filters defined between sessions.

Combined local and remote authentication

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM user accounts for local 5620 SAM authentication with existing TACACS+ or RADIUS user accounts.

Consider the following:

- A system administrator can integrate the existing TACACS+ or RADIUS user accounts with 5620 SAM user accounts.
- You can create a 5620 SAM user name that exactly matches a TACACS+ or RADIUS user name.
- A 5620 SAM user name can be 1 to 80 characters in length, which is sufficient to match most remote authentication user names.

- 5620 SAM users who currently authenticate remotely can log in to the 5620 SAM using their RADIUS or TACACS+ passwords.
- 5620 SAM user authentication requires an account password that observes the 5620 SAM password constraints described in this chapter.

Note — When the samvsa parameter in the 5620 SAM JAAS configuration file is set to true, the 5620 SAM requires a user group from the remote server for authorization and the following conditions apply:

- If a 5620 SAM user account is associated with a local user group and configured to use remote authentication, the local user group is replaced by the remote user group.
- The user group sent by the remote server must exist in the 5620 SAM, otherwise, authentication fails.

The samvsa flag is set to false by default. See "Remote authentication and authorization for users with no 5620 SAM user account" in this chapter and Procedure 9-23 for more information about configuring the 5620 SAM VSA.

For example, a user named jane has the following accounts:

- a remote RADIUS account called jane and the password accessforjane
- a local 5620 SAM account called jane and the password LetJane1In!

When jane is authenticated by RADIUS, she gains access to the 5620 SAM by typing in jane and accessforjane. If the RADIUS server is down, jane is authenticated locally by the 5620 SAM after typing jane and LetJane1In!.

Client session control

Each 5620 SAM GUI client, 5620 SAM-O JMS client, or XML API request creates a 5620 SAM client session. You can view a list of the active 5620 SAM client sessions on the Sessions tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can also terminate one or more 5620 SAM GUI client sessions. When a 5620 SAM GUI client session is terminated in this manner, each client application receives a warning message and the connection is closed by the 5620 SAM server after a short delay.

Messaging connections

A list of active 5620 SAM GUI connections and 5620 SAM-O JMS connections can be viewed on the Messaging Connections tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can terminate one or more connections. When a 5620 SAM-O client connection is terminated, a notification is sent to the 5620 SAM-O client, but the admin user must also remove the 5620 SAM-O JMS client connection so that the server stops storing JMS messages for the session.

Client delegate sessions

The threshold for the number of 5620 SAM client sessions allowed on a client delegate server is configurable using the 5620 SAM GUI. When a user tries to open a client session that exceeds the threshold, the client delegate server opens the session, displays a warning message to the user, and raises an alarm. The threshold-crossing function can help to balance the session load across multiple client delegate servers. You require the Update user permission on the Server package to configure this threshold. See Procedure 9-29 for more information.

9.2 Sample 5620 SAM user authentication configuration

Figure 9-1 shows an example of how 5620 SAM user and user group authentication is performed.

Note 1 — RADIUS and TACACS+ authentication servers support multiple users. If the 5620 SAM cannot reach the first authentication server, the 5620 SAM sequentially attempts the user authentication using the remaining authentication servers.

Note 2 — If user authentication fails against the first authentication server in a sequence (for example, because of wrong password), there is no attempt to authenticate the user against the next authentication server in the sequence.

Note 3 — The EMS server log and 5620 SAM session log record unsuccessful user authentication attempts for known and unknown users. A user that is not defined in the 5620 SAM but belongs to an external AAA server is an example of an unknown user.

Figure 9-1 Sample 5620 SAM user and user group authentication

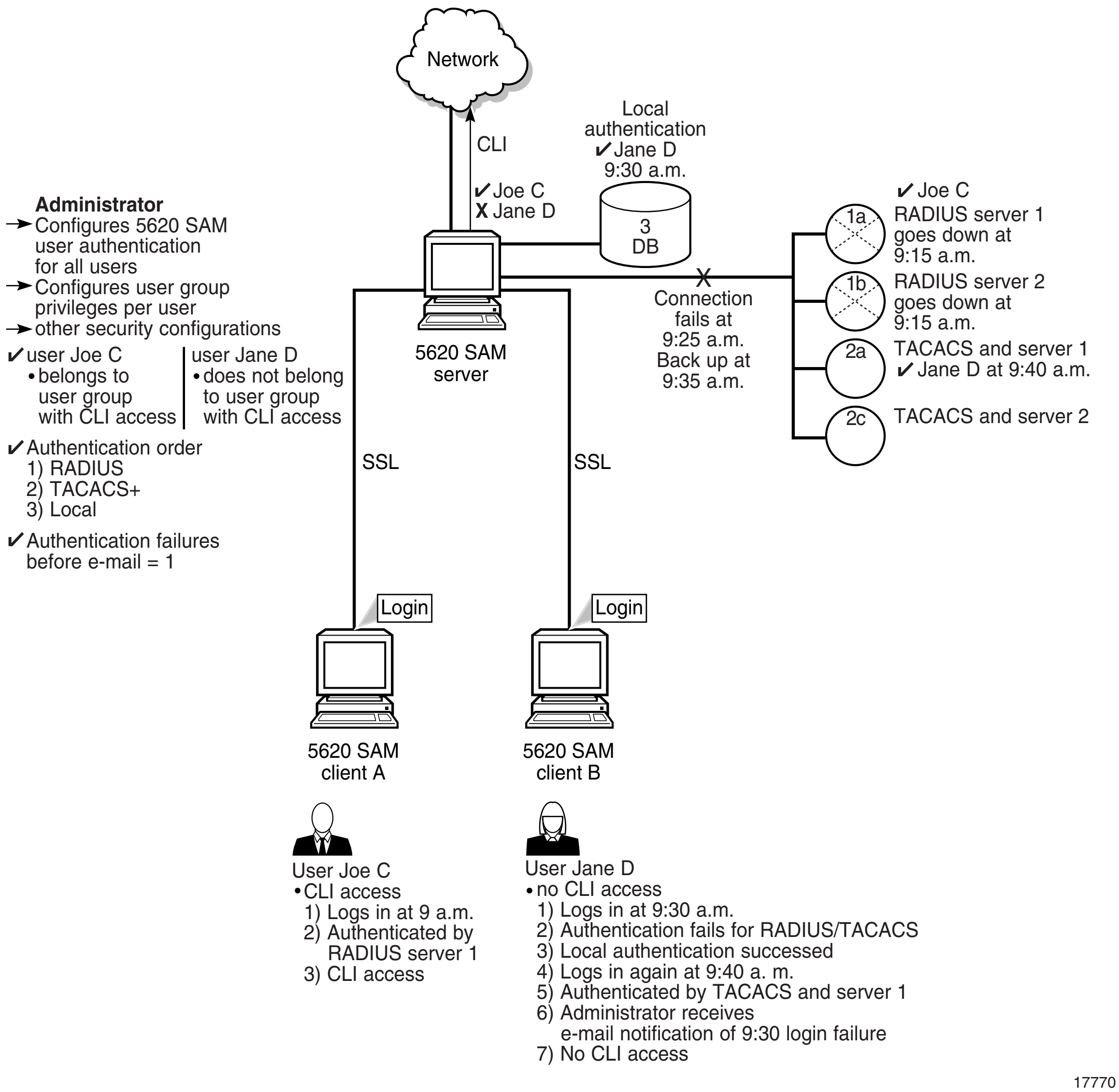


Table 9-3 lists the high-level tasks required to configure this sample.

Table 9-3 Sample 5620 SAM user authentication configuration

Task	Description
Pre-configurations	Ensure proper RADIUS or TACACS+ server configuration, according to your company requirements. PAP authentication is supported for RADIUS and TACACS+. The 5620 SAM server must be able to communicate with the authentication servers to validate users. All configuration tasks should be done with admin access. The 5620 SAM server IP address must be configured as the client of the RADIUS or TACACS+ server. The secret keys must match on the 5620 SAM server and the RADIUS or TACACS+ server.

(1 of 2)

Task	Description
1. Configure the remote authentication order for all users	Choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. Set the authentication order parameters to: • radius • tacplus • local Also specify the RADIUS and TACACS+ servers using the corresponding tabs on the same form.
2. Create scope of command profiles	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI scope of command profile and assign the default CLI management role to the profile. Create at least one scope of command profile that does not allow CLI access by assigning the *default* scope of command role, which has no access permissions to CLI management.
3. Create and configure user groups	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI user group and at least one user group that does not allow CLI access. Assign the scope of command profile with CLI management access to the CLI user group. Assign the scope of command profile with no CLI management access to the user group without CLI access. Authorization is done using user groups, so each user must belong to a user group with a local account on the 5620 SAM server.
4. Create and configure user accounts	You can create local users on the 5620 SAM by performing the following steps, or define remote users using RADIUS and TACACS+. The local users are available when RADIUS or TACACS+ authentication is not available. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create users. Assign the appropriate user group to each user: one with CLI access and one without CLI access.
5.Configure notification	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Configure the authentication failure action parameters, including the parameters that allow the e-mail account of the administrator to be notified after login failure.

(2 of 2)

Consider the following:

- The 5620 SAM server acts as a network access server. A network access server is considered a client of a RADIUS or TACACS+ server.
- The sequence of activity between the 5620 SAM server, which is the authentication client, and the RADIUS or TACACS+ server, which is the authentication server, is the following:
    - client requests authentication
    - server replies to authentication request
    - client requests logout and authentication stops
- When the remote authentication servers are down and local authentication is used, the user must log in using 5620 SAM credentials, as described in "Combined local and remote authentication".

9.3 Sample span rule configuration

This section describes the configuration of a policy that directs the 5620 SAM to automatically add each service created for Customer X to an Edit Access span associated with the service creator. A user named Bob is designated the service administrator for Customer X; only Bob can create or edit Customer X services. A regular service user, by contrast, can only view the Customer X services.

Table 9-4 Sample span rule configuration

Task	Description
1. Create a span that contains the existing Customer X services.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Span on the Span of Control tab. • Specify Customer X Services as the span name. • Use the Contents tab to specify the Customer X services.
2. Create a span of control profile for Bob.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Profile on the Span of Control tab. • Add the Default Service Span as a View Access span to the span of control profile; the user cannot create a new service unless this is done. • Add the Customer X Services span as an Edit Access span to the span of control profile.
3. Create a range policy for each service type that the Customer X service administrator can create; in this sample, the services are IES and VPRN services.	• Choose Administration→Format and Range from the 5620 SAM main menu. • Choose Create→Range Policy. • Specify IES Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Use the Add button on the Users tab to assign the policy to Bob. • Choose Create→Range Policy. • Specify VPRN Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Use the Add button on the Users tab to assign the policy to Bob.
4. Create a span rule that contains the Customer X span.	• Choose Administration→Span Rules from the 5620 SAM main menu. • Specify Customer X Management as the name. • Set the Created In parameter to All listed spans. • Add the Customer X Services span using the Spans tab.

After the span rule is created, Bob creates a new VPRN service for Customer X. The 5620 SAM uses the VPRN range policy to automatically configure the service ID, and applies the associated Customer X Management span rule when Bob saves the service. As a result, the service is added to the Customer X Services span as well as to the Default Service Span. Because Bob has Edit Access to the Customer X Services span, he can reconfigure the service later, as required.

9.4 Workflow to manage 5620 SAM user and group security

1 Assess the requirements for user access to the different 5620 SAM functional areas and develop a strategy for implementing user security. See section 9.1 for more information.

2 Create a proprietary client GUI login screen. See Procedure 9-1 for more information.

3 Reserve a client GUI session for the admin user to ensure that the admin user can always log in. See Procedure 9-2 for more information.

4 Configure user account parameters, as required:

- expiry periods for user account, passwords, and GUI inactivity timeouts; see Procedure 9-3 for more information
- minimum length for user names; see Procedure 9-4 for more information
- user authentication attempts; see Procedure 9-5 for more information
- automated email delivery; see Procedure 9-7 for more information

5 If required, create scope of command roles in addition to the default roles. See Procedure 9-8 for more information.

6 Create scope of command profiles according to types of tasks performed and assign scope of command roles accordingly. See Procedure 9-9 for more information.

7 If required, create spans in addition to the default spans. Add 5620 SAM managed objects to the spans. See Procedure 9-12 for more information.

8 Create span of control profiles and assign spans. See Procedure 9-13 for more information.

9 Create span rules, as required, for automatically assigning new services to spans other than the Default Service Span. See Procedure 9-14 for more information.

10 Create user groups and assign scope of command and span of control profiles to each group, as required. See Procedure 9-17 for more information.

11 Create user accounts for performing the tasks that are assigned to each user group, as defined by the scope of command and span of control profiles associated with each user group. See Procedures 9-18 and 9-19 for more information.

12 Specify 5620 SAM RADIUS and TACACS+ authentication for 5620 SAM user accounts, as required. See Procedure 9-22. See chapter 21 for more information about managing security using RADIUS and TACACS+ authentication.

13 If required, configure authentication and authorization for remote users in which either the 5620 SAM provides the user group to which the user belongs or the remote authentication server provides the user group. See Procedure 9-23 for more information.

14 As required, manage user and group security by performing the following tasks:

- search for inactive user accounts; see Procedure 9-24 for more information
- create, modify and delete user groups; see Procedures 9-17 and 9-20 for more information
- create, modify and delete users; see Procedures 9-18 and 9-21 for more information
- suspend or reinstate users; see Procedures 9-6 and 9-25 for more information
- configure GUI inactivity timeout values; see Procedure 9-3 for more information
- configure password expiry; see Procedure 9-3 for more information

15 Monitor and manage the active client sessions, as required. See Procedures 9-26, 9-27, and 9-28 for more information.

16 As required, manage the user and system logs. See Procedures 9-33, 9-34, and 9-35 for more information.

9.5 5620 SAM user and group security management procedures

This section provides procedures to create and manage users and user groups.

Procedure 9-1 To create a proprietary 5620 SAM login statement

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the security statement parameters:

- Enabled
- Statement

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

The Statement parameter text is displayed on the login form during each subsequent client GUI login attempt.

Procedure 9-2 To reserve an admin account login

You can reserve one client GUI session, from the maximum number of sessions allowed by the license key, for admin users only. This allows an administrator to manage the existing client GUI sessions.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Reserve Administrator Login parameter.

3 Click on the OK button to save the changes and close the form. A dialog box appears.

4 Confirm the action by clicking on the Yes button.

5 Log in as required.

Procedure 9-3 To configure expiry periods and a GUI inactivity timeout

You can configure global expiry periods for user accounts, passwords, and client GUI inactivity checks. You can configure per user group expiry periods for client GUI inactivity checks. You can enable a password history count.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Password History Duration (days) and Password Reuse Cycle parameters.

3 Configure the global expiry period parameters:

- Account Expiry (days)
- Password Expiry (days)
- Client Timeout (minutes)
- Advance Password Expiry Notification (days)

If you set any of the parameters to 0, the corresponding expiry period check is disabled. To change the client inactivity check timeout for individual user groups, see Procedure 9-17.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 9-4 To configure the minimum allowable user name length

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 In the User Name panel, check the Enable box.

3 Configure the Minimum User Name Length Allowed parameter. Select a range between 5 to 40 characters, the minimum is 5 characters.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

Procedure 9-5 To configure authentication failure actions

You can specify an authentication message or a lockout for a user account that exceeds the configured number of login authentication attempts. Only non-admin accounts can be locked out, as admin accounts always have access.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the authentication failure action parameters:

- Attempts before lockout
- Attempts before e-mail
- E-mail Subject
- E-mail text

If you set the Attempts before lockout parameter to 0, the lockout function is disabled.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

Procedure 9-6 To configure suspended account actions

You can specify a suspended account message for a user account when you suspend the user account using the User State parameter.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the suspended account parameters:

- E-mail Subject
- E-mail text

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

Procedure 9-7 To configure automated e-mail delivery

Perform this procedure to specify the e-mail parameters for automated 5620 SAM messages to users and administrators; for example, when locking out a user account that exceeds the allowed number of authentication attempts.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the outgoing e-mail server SMTP parameters:

- Server
- E-mail User Name
- E-mail User Password
- E-mail Address

4 Configure the Test Message parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

Procedure 9-8 To create a scope of command role

Perform this procedure to create a set of user permissions that define an operator role. You can apply one or more scope of command roles to a user group using a scope of command profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Click on the Create button and choose Role. The Role (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Role ID
- Role Name
- Description

5 Perform the following steps to configure the permissions for the scope of command role.

i Click on the Permissions tab button. A list of the 5620 SAM packages, methods, and classes is displayed.

Note — When you enable the Create permission for a 5620 SAM package, method, or class, the Update/Execute permission is automatically enabled.

When you enable the Update/Execute permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

ii Select the required access permissions, which are displayed in the list column headings, for each package, class, or method that you want to assign to the scope of command role.

6 Click on the OK button. The Role (Create) form closes.

7 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-9 To create a scope of command profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Click on the Create button and choose Profile. The Scope of Command Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more scope of command roles to the profile.

i Click on the Roles tab button.

ii Click on the Add button. The Select Role - Role form opens.

iii Select one or more roles and click on the OK button. The Select Role - Role form closes and a dialog box appears.

iv Click on the OK button.

v Click on the OK button. The Scope of Command Profile (Create) form closes.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-10 To delete a scope of command role

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Role (Security) from the object drop-down list and click on the Search button. A list of scope of command roles is displayed.

4 Select a role in the list and click on the Delete button. A dialog box appears.

Note 1 — You cannot delete a predefined scope of command role.

Note 2 — You cannot delete a scope of command role that is assigned to a scope of command profile when the scope of command profile is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the scope of command role.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-11 To delete a scope of command profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Profile (Security) from the object drop-down list and click on the Search button. A list of scope of command profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a scope of command profile that is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the scope of command profile.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-12 To create a span of control

Perform this procedure to specify a set of 5620 SAM objects in a span of control and the type of user access available for the objects. You can apply one or more spans to a user group using a span of control profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Click on the Create button and choose Span. The Span (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Span ID
- Span Name
- Description

5 Click on the Contents tab button.

6 Click on the Add button and choose an object type from the menu. The Select *(object_type)* list form opens.

7 Select one or more objects and click on the OK button. The Select *(objects)* list form closes and the objects are listed on the Span (Create) form. A dialog box appears.

8 Click on the OK button. The Span (Create) form closes.

9 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-13 To create a span of control profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Span of Control tab button.

3 Click on the Create button and choose Profile. The Span of Control Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more spans to the profile.

i Click on the Spans tab button. The predefined spans are listed.

ii Click on the Add button and choose an access type. The Select *access_type* Spans form opens.

iii Select one or more spans in the list and click on the OK button. The Select *access_type* Spans form closes, and a dialog box appears.

iv Click on the OK button. The spans are listed on the Span of Control Profile (Create) form with the type of access displayed in the Access Type column.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-14 To create a span rule

Perform this procedure to create a span rule. A span rule is a policy that specifies to which span of control profiles, in addition to the Default Service Span, a newly created 5620 SAM service is automatically assigned.

1 Using an account with an assigned security scope of command role, choose Administration→Span Rules from the 5620 SAM main menu. The Span Rules form opens.

2 Click on the Create button. The Service Creation Span Rule (Create) form appears.

3 Configure the parameters:

- Auto-Assign ID
- Span Rule ID
- Name
- Created In

4 Perform the following steps to associate one or more spans with the rule.

i Click on the Spans tab button.

ii Click on the Add button. The Select Span(s) form opens.

iii Select one or more spans in the list.

iv Click on the OK button. The Select Span(s) form closes and the selected spans are listed on the Service Creation Span Rule (Create) form.

5 Perform the following steps to associate one or more format or range policies with the rule.

i Click on the Format and Range Policies tab button.

ii Click on the Add button. The Select Format or Range Policies form opens.

iii Select one or more policies in the list.

iv Click on the OK button. The Select Span(s) form closes and the selected policies are listed on the Service Creation Span Rule (Create) form.

6 Click on the OK button. The Service Creation Span Rule (Create) form closes.

Procedure 9-15 To delete a span of control

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Choose Span (Security) from the object drop-down list and click on the Search button. A list of spans is displayed.

4 Select a span in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a default span, or a span in a span of control profile that is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the span of control.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-16 To delete a span of control profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Choose Profile (Security) from the object drop-down list and click on the Search button. A list of span of control profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a span of control profile that is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the span of control profile.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-17 To create a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab button.

3 Perform one of the following:

a Create a new group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed.

b Modify an existing group by performing the following steps.

i Set the filter criteria.

ii Click on the Search button. A list of groups is displayed.

iii Select a group in the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Maximum User Sessions Allowed
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

5 If the user group is intended for use by remote users, configure the parameters:

- Maximum GUI Sessions Allowed
- Maximum OSS Sessions Allowed
- Priority

6 Perform the following steps to assign a scope of command profile to the user group.

i Click on the Select button in the Scope of Command panel. The Select Scope of Command Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Scope of Command Profile form closes, and the User Group (Create) form displays the scope of command profile name.

7 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button in the Span of Control panel. The Select Span of Control Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Span of Control Profile form closes, and the User Group (Create) form displays the span of control profile name.

8 If you are creating a new user account, perform the following steps.

i Click on the OK button. The User Group (Create) form closes.

ii Go to step 15.

9 Click on the Format and Range Policies tab button.

10 Click on the Add button. The Select Format or Range Policies form opens.

11 Select one or more policies in the list and click on the OK button.

12 Click on the OK button. A dialog box appears.

Note — When you change the scope of command or span of control profiles of a group, the permissions of each user in the group are altered immediately when you click on the OK button.

13 Click on the Yes button. The User Group (Create) form closes.

14 If an active client GUI session is affected by the user group modification, restart the GUI client.

15 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-18 To create a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Perform one of the following:

a Create a new user account by clicking on the Create button. The User (Create) form opens with the General tab displayed.

b Modify an existing user account by performing the following steps.

i Set the filter criteria.

ii Click on the Search button. A list of user accounts is displayed.

iii Select an account in the list and click on the Properties button. The User (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- User Name
- Description
- User State
- E-mail Address
- Priority
- Password Change Required
- User Password
- Confirm Password
- Maximum Sessions Allowed
- Maximum OSS Sessions Allowed
- Valid Client IP address
- Enable IP Address validation

Note — If the user account is for a remote user, you cannot configure the Maximum Sessions Allowed, Maximum OSS Sessions Allowed, or Priority parameters. For remote users, these parameters are derived from the user group configured on the user account.

5 You can test the validity of the user e-mail address by clicking on the Test E-mail button beside the E-mail Address parameter.

Note — Before you test the validity of the user e-mail address, ensure that the outgoing SMTP e-mail server and e-mail test message are configured. See Procedure 9-7 for information about configuring the outgoing e-mail server and test message.

6 Perform the following steps to choose a user group for the user account.

i Click on the Select button. The groupName form opens.

ii Select a user group in the list and click on the OK button. The groupName form closes, and the User (Create) form displays the user group name.

7 If you are creating a new user account, perform the following steps.

   i Click on the OK button. The User Group (Create) form closes.

   ii Go to step 13.

8 Click on the Format and Range Policies tab button.

9 Click on the Add button. The Select Format or Range Policies form opens.

10 Select one or more policies in the list and click on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The User (Edit) form closes.

13 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-19 To copy a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Set the filter criteria and click on the Search button. A list of configured users opens.

4 Choose a user from the list and click on the Properties button. The User *type_of_user*, Group *user_group* (Edit) form opens.

5 Click on the Copy button. A User (Create) form opens for the second user.

6 Configure the parameters, as required. You must change the User Name parameter and configure the User Password and Confirm Password parameters.

7 Click on the OK button to save the changes and close the form.

8 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-20 To delete a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab button.

3 Configure the filter criteria and click on the Search button. A list of user groups is displayed.

4 Select a group in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the user group.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-21 To delete a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab button.

3 Configure the filter criteria and click on the Search button. A list of user accounts is displayed.

4 Select an account in the list and click on the Delete button. A dialog box appears.

Note — When a user account is associated with a scheduled task, you must decide whether to remove the schedules. If you do not want to remove the schedules, no schedules are removed. If you do want to remove schedules, the schedules associated with the user account are removed if the schedule is not associated with a scheduled task. Schedules that are associated with a scheduled task are not removed.

5 Click on the Yes button. The 5620 SAM deletes the user account.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 9-22 To create RADIUS and TACACS+ authentication policies for 5620 SAM user accounts

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. The RemoteAuthenticationManager (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Authentication Order 1
- Authentication Order 2
- Authentication Order 3

3 Click on the RADIUS tab button to configure RADIUS authentication server parameters.

4 Click on the Create button. The SAM RADIUS Authentication Server (Create) form opens.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Port
- Retry Attempts
- Timeout (seconds)
- Secret Name

6 Click on the OK button to save the changes.

7 Verify the action.

8 Click on the TACACS tab button to configure TACACS+ authentication server parameters.

9 Click on the Create button. The SAM TACACS+ Authentication Server (Create) form opens.

10 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Timeout (seconds)
- Secret Name

11 Click on the OK button to save the changes.

12 Verify the action.

13 Click on the Faults tab to view alarms, as required.

14 Click on the OK button to save the changes and close the form.

Procedure 9-23 To configure remote authentication and authorization for remote-only users

Note 1 — Ensure that remote authentication is enabled. See Procedure 9-22 for information about creating RADIUS and TACACS+ authentication policies.

Note 2 — See "Remote authentication and authorization for users with no 5620 SAM user account" in section 9.1 for information about remote authentication and authorization for remote-only users.

1 Perform one of the following:

a To configure remote authentication and authorization for remote-only users where the 5620 SAM provides the user group to which the user belongs, go to step 2.

Note — The samvsa flag must be set to false in the SamJaasLogin.config file. The default value is false. The SamJaasLogin.config file is located in the server installation configuration directory, typically C:\5620sam\client\nms\config or /opt/5620sam/server/nms/config.

b To configure remote authentication and authorization for remote-only users where the remote authentication server provides the user group to which the user belongs, go to step 3.

2 Specify the default external user group.

i Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

ii Configure the default external user group parameter: User Group.

iii Click on the Select button. The Select Group - TSecurityManager form opens.

iv Select a user group and click on the OK button. The Select Group - TSecurityManager form closes and the 5620 SAM User Security - Security Management (Edit) form refreshes with the selected user group.

Note — Do not select a user group that has the Apply Local Authentication Only parameter enabled. Doing so may cause subsequent login attempts to fail once the user is created locally in 5620 SAM.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

3 Modify the SamJaasLogin.config file.

Note — Ensure that you create a backup of the SamJaasLogin.config file before you make any modifications to it.

i Log in to the 5620 SAM main server station as the samadmin user.

ii Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

iii Open the SamJaasLogin.config file using a text editor.

iv If RADIUS authentication is enabled, find the RADIUSLogin section of the file and change the samvsa flag to true. The following is an example of the file text:

```
RADIUSLogin
{
  com.timetra.nms.jaas.provider.radius.auth.RadiusJaasLoginM
odule REQUIRED
debug=false
  samvsa=true
;
};
```

If TACACS+ authentication is enabled, find the TACACSLogin section of the file and change the samvsa flag to true. The following is an example of the file text:

```
TACACSLogin
{
  com.timetra.nms.jaas.provider.tacacs.auth.TacacsPlusJaasLo
ginModule REQUIRED
debug=false
  samvsa=true
;
};
```

v Save the file.

vi Close the file.

vii Enter the following at the CLI prompt:

```
bash$ path/nms/bin/nmsserver.bash read_config ↵
```

where
path is the 5620 SAM server installation location, typically opt/5620sam/server

The 5620 SAM server puts the configuration changes into effect.

4 Define the user group VSA on the remote authentication server.

Note — Step 4 must be performed by the remote authentication server administrator.

Perform one of the following:

a If RADIUS authentication is enabled:

i Copy the example of the RADIUS dictionary below to the RADIUS dictionary file. Enter changes to the file based on your RADIUS configuration.

ii Configure the RADIUS user profile and add a previously defined 5620 SAM user group name to the Sam-security-group-name VSA. The following is an example of the RADIUS user group VSA:

```
Sam-security-group-name="user_group_name_locally_defined
_in_5620SAM"
```

The VSA configuration file contains information such as usernames, passwords, and the 5620 SAM user group name. The user authentication process returns the user group name in the Sam-security-group-name VSA of the access-accept message.

The following is an example of the RADIUS dictionary text:

```
##########################################################
###
#           Alcatel-Lucent 5620 SAM Server
dictionary.    #
#  $Id: dictionary.alcatel.sam,v
1.1 2006/08/18 10:00:22$ #
##########################################################
####

VENDOR          Alcatel-Lucent                      123

BEGIN-VENDOR                             Alcatel-Lucent

ATTRIBUTE       Sam-security-group-name      3       stri
ng

END-VENDOR                               Alcatel-Lucent
```

Note 1 — The user group must be a valid user group in the 5620 SAM.

Note 2 — The vendor ID must be 123.

b If TACACS+ authentication is enabled, define the 5620 SAM user group VSA in the user profile on the TACACS+ server. The following is an example of the TACACS+ user group VSA:

```
service=sam-app{
  sam-security-group="user_group_name_locally_defined_in_562
0SAM"
}
```

Note — The user group must be a valid 5620 SAM user group.

Procedure 9-24 To search for inactive user accounts

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab button.

3 Click on the Inactive User Search button and perform one of the following.

- **a** Choose 90 Days.
- **b** Choose 180 Days.
- **c** Choose Custom. The User Inactivity Period form opens.
    - **i** Configure the User inactive greater than or equal to parameter.
    - **ii** Click on the OK button to close the form and return to the Inactive User Search form.

4 User accounts that have been inactive for a number of days that is greater than or equal to the value entered in step 3 are displayed.

5 Perform actions for inactive user accounts, as required.

Procedure 9-25 To suspend or reinstate a 5620 SAM user account

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Suspend or reinstate the user.

   a To suspend the user, set the User State parameter to suspended.

   b To reinstate the user, set the User State parameter to active.

7 Click on the Apply button to save the changes.

8 Verify the action.

9 Close the form.

Procedure 9-26 To administratively change the password of a 5620 SAM user

The system administrator uses the Security Management form to maintain user accounts. The user can change their password in a separate form. If a user forgets their password, the system administrator can change the password and inform the user of the new password.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Configure the User Password parameter and the Confirm Password parameter.

7 Click on the Apply button to save the changes.

8 Verify the action.

9 Close the form.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 9-27 To request a password change for a 5620 SAM user

The system administrator uses the Security Management form to maintain user accounts. The system administrator can request a password change for a specific 5620 SAM user. The user can change their password in a separate form.

Note — This change does not affect the current user session.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Enable the Password Change Required check box to request a password change for the user.

7 Click on the Apply button to save the changes.

8 Verify the action.

9 Close the form.

The next time the user logs in to 5620 SAM, the user will be prompted to change his or her password. Once the user changes his or her password, the Password Change Required check box returns to the default of unchecked.

Procedure 9-28 To change the password of the current 5620 SAM user

Users change their password in the Change Password form.

1 Start the 5620 SAM and log in using your user name and password.

2 Choose Administration→Security→Change Password from the 5620 SAM main menu. The Password Change form opens.

3 Verify that the Login Name matches your user account name.

4 Configure the parameters:

- Old Password
- New Password
- Confirm Password

5 Click on the OK button to save the changes.

6 Confirm the action, as required.

7 Close the form.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 9-29 To configure the number of allowed client sessions for a client delegate server

Note — The 5620 SAM continues to accept new client sessions from a client delegate server after the allowed number of sessions is reached. The maximum number of sessions is to be used as a guide for balancing the client session load among multiple client delegate servers.

1 Using an account with Update permission on the Server package, choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

2 Click on the Client Delegate Servers tab button.

3 Specify a filter and click on the Search button. A list of client delegate servers is displayed.

4 Select an entry in the list and click on the Properties button. The Client Delegate Server (Edit) form opens.

5 Configure the Maximum UI Sessions parameter.

6 Click on the OK button. The Client Delegate Server (Edit) form closes and the System Information form reappears.

7 Closes the System Information form.

Procedure 9-30 To view and manage the active 5620 SAM client sessions

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab button.

3 Specify a filter to create a filtered list of GUI or 5620 SAM-O JMS client sessions and click on the Search button. The list of currently active client sessions opens.

4 Review the following session information:

- user name logged in for the client GUI session
- ID of the session
- time and date that the session started
- user group privileges for the session
- type of client, either a GUI (5620 SAM) or 5620 SAM-O JMS (SAMOSS) client
- IP address of the client

5 Perform one of the following:

a Close the form.

b Choose a session from the list and click on the Close Session button to shut down the client session.

Note — There are additional dependencies for closing a 5620 SAM-O session. See Procedure 9-32 for more information.

6 Validate the action.

7 Close the form.

Procedure 9-31 To send a text message to 5620 SAM GUI users

Administrative users can send broadcast messages to some or all active GUI users logged into the 5620 SAM. This is useful for sending maintenance and similar notifications to active users.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab button.

3 Specify a filter to create a filtered list of GUI client sessions and click on the Search button. A list of active client sessions is displayed.

4 Select the required client sessions in the list.

5 Click on the Text Message button. The Text Message form opens.

6 Enter your text message in the Text Message form and click on OK. The text message is sent to the selected clients.

7 Close the Security Management (Edit) form.

Procedure 9-32 To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Messaging Connections tab button.

3 Specify a filter to create a filtered list 5620 SAM-O JMS client connections and click on the Search button. The list of currently active client connections opens.

4 Perform one of the following:

a Choose a JMS connection from the list and click on the Close Connection button to shut down the client connection. The connection to the server is terminated when you close a durable JMS connection, however, the subscription continues to store JMS messages.

b Choose a JMS connection from the list and click on the Remove Connection button to shut down the client connection and remove the durable subscription. The server stops storing the JMS messages for the session.

Note — When you remove a durable subscription, the OSS client can still attempt to connect to the 5620 SAM-O server. You can prevent an OSS client from attempting to connect by suspending the OSS user account. See Procedure 9-25 for more information.

5 Validate the action.

6 Close the form.

Procedure 9-33 To view client usage and activity logs

Perform this procedure to view client activity log entries to identify the 5620 SAM user and action associated with a network problem. Activity log collection is enabled by default. See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using the 5620 SAM client activity log.

Note — A user with LI privileges can see and access LI-related activity and usage records. A 5620 SAM user with appropriate access can see all non-LI related activity and usage records.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Choose a type of user log from the object drop-down list:

- Database Log to view information about changes to the database due to actions performed by the client
- Deployment Log to view information about deployment requests sent from the client
- Session Log to view information about the current client session, including operations performed and permissions for the logged in user account
- User Read Log to view information about data viewed by users of the client
- User Request Log to view information about user requests sent from the client

3 Specify a filter to create a filtered list of logs, and click on the Search button. The list of logs opens.

4 To edit the log, choose a log from the list and click on the Properties button. The log opens. Review the log information. See the *5620 SAM Troubleshooting Guide* for more information about reading and interpreting logs.

The information displayed depends on the type of log. For example, user read logs display:

- username logged in for the client session
- timestamp information
- type of operation performed; for example, configuration
- user account name that performed the operation
- target class against which the operation was performed
- information about the actions performed, based on the log type

When you are finished editing the log, click on the Close button to close the log.

5 Click on the Close button to close the 5620 SAM Usage and Activity Records form.

Procedure 9-34 To save activity or usage logs to a file

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Choose a type of user log from the object drop-down list:

- Database Log to view information about changes to the database due to actions performed by the client
- Deployment Log to view information about deployment requests sent from the client
- Session Log to view information about the current client session, including operations performed and permissions for the logged-in user account
- User Read Log to view information about data viewed by users of the client
- User Request Log to view information about user requests sent from the client

3 Specify a filter to create a filtered list of logs, and click on the Search button. The list of logs opens.

4 Highlight the log records that appear in the search list.

5 Right-click on a column heading and choose Save to File from the contextual menu. The Save As form appears.

6 Save the results.

i To choose a directory in which to save the listed information, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose HTML or CSV from the File of Type drop-down menu.

iv Click on the Save button. The results of the inventory search are saved to the specified HTML or CSV file.

7 Close the 5620 SAM Usage and Activity Records form.

Procedure 9-35 To configure client usage and activity logging

Perform this procedure to configure how the 5620 SAM logs client activity. Activity log entries can identify the 5620 SAM user and action associated with a network problem. Activity log collection is enabled by default. See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using the 5620 SAM client activity log.

Note — A user with LI privileges can see and access LI-related activity and usage records. A 5620 SAM user with appropriate access can see all non-LI related activity and usage records.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Choose a type of user log from the object drop-down list:

- Database Log to view information about changes to the database due to actions performed by the client
- Deployment Log to view information about deployment requests sent from the client
- Session Log to view information about the current client session, including operations performed and permissions for the logged-in user account
- User Read Log to view information about data viewed by users of the client
- User Request Log to view information about user requests sent from the client

3 Click on the Log Policy button to specify how much data to collect and store in the log or whether to turn logging off. The appropriate logger configuration form opens.

i Configure the parameters:

- Retention Time (hours)
- Administrative State

Click on the Apply button to save the changes.

ii Click on the Purge Log Records button to delete log records. Log records that meet storage specifications are stored and can be viewed. See the *5620 SAM Statistics Management Guide* for more information.

iii Click on the OK or Cancel button to close the Edit Policy form.

4 Click on the Close button to close the 5620 SAM Usage and Activity Records form.

10 — 5620 SAM SSL security

10.1 5620 SAM SSL security overview

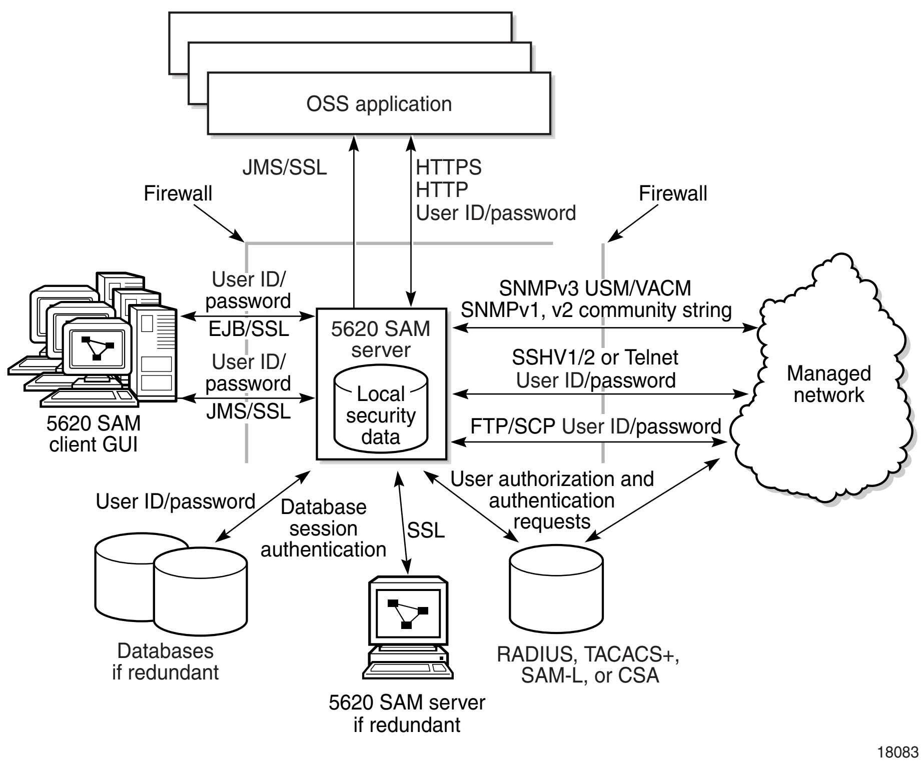
Secure Sockets Layer, or SSL, is a security mechanism for data encryption, client authentication, and message integrity. You can configure SSL for secure communication between 5620 SAM main servers and other 5620 SAM components such as GUI and OSS clients, client delegate servers, and auxiliary servers.

Note — You cannot selectively enable SSL on the components in a 5620 SAM system. If you enable SSL on a main server, you must enable SSL in all other 5620 SAM server and client configurations.

SSL secures the EJB, JMS, and HTTP interfaces of 5620 SAM single-user GUI clients and client delegate servers, and the JMS and HTTP interfaces of OSS clients. When SSL is enabled on a 5620 SAM GUI or OSS client, the client uses HTTPS instead of HTTP.

Figure 10-1 shows the communication channels between 5620 SAM components.

Figure 10-1 5620 SAM communication channels and security



SSL requires a security certificate that is shared among members of a network domain. The certificate can be generated locally, or obtained from a certification authority, or CA. A locally generated certificate, which is called a self-signed certificate, is for use only in a private network.

SSL security certificates are stored in a keystore file on a 5620 SAM main server. A truststore file, which is also stored on a main server, contains SSL security certificates from trusted entities.

You can enable 5620 SAM SSL by specifying the keystore and truststore files during a 5620 SAM installation or upgrade, or by using the 5620 SAM configuration utility on an installed system. If SSL is configured and enabled on a 5620 SAM Release 9.0 or later system, the SSL configuration is maintained through subsequent upgrades.

A 5620 SAM server can act as an SSL client to another server. For example, in a redundant 5620 SAM deployment, the standby main server is an SSL client of the primary main server. Also, when SSO is configured, a 5620 SAM main server keystore must contain the SSL certificate of the remote server.

A main server automatically distributes the truststore file to each 5620 SAM GUI client. However, you must manually copy the truststore file to the other main server in a redundant deployment, and to each auxiliary server and OSS client in the 5620 SAM system.

Note 1 — To enable or disable SSL on a single-user GUI client or delegate client, you must uninstall the single-user client or client delegate server software, and then select the appropriate SSL option during the client or client delegate server re-installation. A GUI client cannot connect to a main server that has a different SSL configuration, so the main server cannot update the client SSL configuration.

Note 2 — Alcatel-Lucent recommends using the Java Key Store, or JKS, keystore format in a 5620 SAM system. If you have a keystore in a different format, for example, PKCS12, you can use the Java keytool utility to convert the keystore to JKS format, as described at the following location:

http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

10.2 Workflow to configure SSL for a 5620 SAM system

Caution 1 — Configuring SSL in a standalone 5620 SAM system requires a shutdown of the main server, which causes a network management outage. Configure SSL in a 5620 SAM system only during a scheduled maintenance period.

Caution 2 — Configuring SSL in a redundant 5620 SAM system requires a server activity switch, which causes a network management outage. Configure SSL in a 5620 SAM system only during a scheduled maintenance period.

1 Prepare the required keystore and truststore files. See Procedure 10-1 for more information.

i If you do not want to use a self-signed security certificate, request a security certificate from a CA.

ii If you use a self-signed security certificate, generate an SSL keystore file.

iii If the security certificate in the keystore file is self-signed, export the certificate to a certificate file.

iv Import the self-signed or CA certificate from the certificate file to the default truststore file on the main server.

v Copy the truststore file from the main server station to the following stations in the 5620 SAM system:

- the other main server station in a redundant deployment
- each auxiliary server station
- each OSS client station

2 If the 5620 SAM system is deployed in a redundant configuration, enable SSL on the standby main server. See Procedure 10-2 for more information.

3 Enable SSL on each reserved auxiliary server. See Procedure 10-3 for more information.

4 If the 5620 SAM system includes multiple GUI clients, enable SSL on one GUI client or client delegate server to minimize the loss of network visibility during the required server activity switch. See Procedures 10-4 and 10-5 for more information.

5 If the 5620 SAM system is deployed in a redundant configuration, enable SSL on the primary main server. See Procedure 10-2 for more information.

6 If the 5620 SAM system is deployed in a standalone configuration, enable SSL on the standalone main server. See Procedure 10-2 for more information.

7 Enable SSL on each preferred auxiliary server. See Procedure 10-3 for more information.

8 Enable SSL on the remaining GUI clients and client delegate servers. See Procedures 10-4 and 10-5 for more information.

9 Enable HTTPS on each OSS client. See Procedure 10-6 for more information.

10.3 SSL configuration procedures

The following procedures describe how to configure and enable SSL in a 5620 SAM system.

Procedure 10-1 To prepare a 5620 SAM system for SSL configuration

Perform this procedure to create the keystore and truststore files required for SSL security in a 5620 SAM system.

Caution — Alcatel-Lucent strongly recommends that you obtain an SSL security certificate from a CA.

Note — The Solaris keytool command-line options specified in this procedure are the basic options required to generate a CSR, generate a keystore file, and import and export certificates. Visit the following URL for information about the available command-line options:

http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

1 Log on to a 5620 SAM main server station as the samadmin user.

2 Open a console window.

3 Navigate to the *path*/jre/bin directory.

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

4 Perform one of the following to generate a keystore file using the keytool utility.

a Generate a keystore file that contains a security certificate from a CA.

i Enter the following to generate a certificate signing request, or CSR:

```
bash$ ./keytool -certreq -alias alias -sigalg sigalg
-file certreq_file -keypass keypass -storetype JKS
```

where
alias is a case-insensitive alias that is required for subsequent keytool operations
sigalg is the encryption algorithm for signing the CSR, such as SHA or RSA
certreq_file is the output file that is to contain the CSR
keypass is the password to assign to the keystore

ii Send the generated CSR file to a CA. The CA authenticates the certificate requestor and returns a certificate or certificate chain, which is used to replace the existing certificate chain in a keystore.

b Generate a keystore file that contains a self-signed security certificate.

i Enter the following to generate a keystore file:

```
bash$ ./keytool -genkey -alias alias -keyalg RSA -keypass
password -storepass password -keystore destination_file
-validity days -dname "CN=common_name, OU=org_unit,
O=org_name, L=locality, S=state, C=country" ↵
```

where
alias is a case-insensitive alias that is required for subsequent keytool operations
password is a password used to secure the key and keystore
destination_file is the path and name of the keystore file
days is the number of days before the SSL key expires; the default is 90 if the -validity option is not specified
and where the following comprise the X.500 distinguished name:
common_name is the name of a person
org_unit is a department or division name
org_name is a company name
locality is a city name
state is a state or region name
country is a country code, for example, US

The following is an example keystore generation command:

```
./keytool -genkey -alias bob -keyalg RSA -keypass
BobsPassword -storepass
BobsPassword -keystore /opt/samserver.keystore -validity
365 -dname "CN=Bob Smith, OU=Accounting, O=ABC Inc.,
L=Pittsburgh, S=Pennsylvania, C=US"
```

In this example, the utility creates the /opt/samserver.keystore file, which contains the SSL key. The key is valid for 365d, or one year.

ii Record the keystore password.

iii Enter the following to export the certificate from the keystore file to a certificate file:

bash$ **./keytool -export -alias *alias* -keystore *keystore_file* -storepass *password* -file *certificate_file*** ↵

where
alias is the keystore alias specified during keystore generation
keystore_file is the generated keystore file, for example, /opt/samserver.keystore
password is the keystore password
certificate_file is the path and name of the certificate file to create

5 Enter the following to import the certificate from the certificate file to a truststore file on the main server:

Note — You can import the certificate to the default 5620 SAM truststore file, or to an existing truststore file. The default 5620 SAM truststore file is *path*/nms/config/ssl/trustStore/cacerts.trustStore, where *path* is the 5620 SAM server installation directory, typically /opt/5620sam/server.

bash$ **./keytool -importcert -trustcacerts -alias *alias* -file *certificate_file* -keystore *truststore_file* -storepass *password***

where
alias is the keystore alias
certificate_file is the self-signed or CA certificate file
truststore_file is the truststore file to which you want to import the certificate
password is the truststore password

6 Copy the truststore file from the main server station to the following stations in the 5620 SAM system:

Note — You must copy the truststore file to the same location on each station in the system, for example, /opt.

- the other main server station in a redundant deployment
- each auxiliary server station
- each OSS client station

Procedure 10-2 To enable SSL on a main server

Perform this procedure to enable SSL encryption on a 5620 SAM main server for communication with other 5620 SAM components.

Caution — Configuring SSL on a 5620 SAM main server requires a shutdown of the server software and causes a network-management outage. Ensure that you perform this procedure only during a scheduled maintenance period.

Note — You must perform this procedure on each main server In a redundant 5620 SAM deployment. See section 10.2 for information about the order in which the main servers must be configured.

1 Stop the 5620 SAM main server application.

i Log in to the main server station as the samadmin user.

ii Open a console window.

iii Enter the following to change to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iv Enter the following to stop the 5620 SAM main server software:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the 5620 SAM main server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

vi The 5620 SAM main server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays a different message, wait 5m and repeat step 1 v. Do not proceed to the next step until the server is stopped.

2 Enter the following to switch to the root user:

```
bash$ su - ↵
```

3 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

4 Navigate to the DVD-ROM drive.

5 Perform one of the following to open the 5620 SAM server installer.

a On a SPARC station:

i Enter the following:

```
# cd Solaris ↵
```

ii Enter the following:

```
# ./ServerInstall_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On an x86-based station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./ServerInstall_x86_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

6 Click on the Next button.

7 Accept the terms of the license agreement in the “Software License Agreement” panel.

8 Click on the Next button.

9 Choose Main Server Configuration in the “Choose Installation Type” panel.

10 Click on the Next button.

11 Click on the Next button in each subsequent panel until the “SSL Configuration” panel is displayed.

12 Select the “Enable Secure Communication” parameter.

13 Configure the remaining parameters:

- Keystore File
- Keystore Password
- Truststore File
- Truststore Password

14 Click on the Next button.

15 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

16 Select the “Start the 5620 SAM Main Server” parameter.

17 Click on the Done button to close the server configuration utility.

18 Enter the following to switch back to the samadmin user:

exit ↵

19 Close the console window.

Procedure 10-3 To enable SSL on an auxiliary server

Perform this procedure to enable SSL encryption on a 5620 SAM auxiliary server for communication with other 5620 SAM components.

1 Stop the 5620 SAM auxiliary server application.

i Log in to the auxiliary server station as the samadmin user.

ii Open a console window.

iii Enter the following to change to the server binary directory:

bash$ **cd *path*/nms/bin** ↵

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/auxserver

iv Enter the following to stop the 5620 SAM auxiliary server software:

bash$ **./auxnmsserver.bash auxstop** ↵

v Enter the following to display the 5620 SAM auxiliary server status:

bash$ **./auxnmsserver.bash auxappserver_status** ↵

The command displays a status message.

vi The auxiliary server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays a different message, wait 5m and repeat step 1 v. Do not proceed to the next step until the server is stopped.

2 Enter the following to switch to the root user:

bash$ **su -** ↵

3 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

4 Navigate to the DVD-ROM drive.

5 Perform one of the following to open the 5620 SAM server installer.

a On a SPARC station:

i Enter the following:

\# **cd Solaris** ↵

ii Enter the following:

\# **./ServerInstall_SAM_9_0_*revision*.bin** ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On an x86-based station:

i Enter the following:

\# **cd Solarisx86** ↵

ii Enter the following:

\# **./ServerInstall_x86_SAM_9_0_*revision*.bin** ↵

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

6 Click on the Next button.

7 Accept the terms of the license agreement in the “Software License Agreement” panel.

8 Click on the Next button.

9 Choose Auxiliary Server Configuration in the “Choose Installation Type” panel.

10 Click on the Next button.

11 Click on the Next button in each subsequent panel until the “SSL Configuration” panel is displayed.

12 Select the “Enable Secure Communication” parameter.

13 Configure the remaining parameters:

- Truststore File
- Truststore Password

14 Click on the Next button.

15 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

16 Select the “Start the 5620 SAM Auxiliary Server” parameter.

17 Click on the Done button to close the server configuration utility.

18 Enter the following to switch back to the samadmin user:

```
# exit ↵
```

19 Close the console window.

Procedure 10-4 To enable SSL on a Solaris GUI client or client delegate server

Perform this procedure to enable SSL on a 5620 SAM single-user GUI client that runs on Solaris, or on a client delegate server.

Note — To enable or disable SSL on a single-user GUI client or delegate client, you must uninstall the single-user client or client delegate server software, and then select the appropriate SSL option during the client or client delegate server re-installation. A GUI client cannot connect to a main server that has a different SSL configuration, so the main server cannot update the client SSL configuration.

1 Close the client GUI, if it is open, by choosing Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The client GUI closes.

3 Uninstall the client or client delegate server by performing the appropriate procedure in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

4 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

5 Open a console window.

6 Navigate to the DVD-ROM drive.

7 Perform one of the following to open the 5620 SAM client installer.

a On a SPARC station:

i Enter the following:

```
# cd Solaris ↵
```

ii Enter the following:

```
# ./ClientInstall_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On an x86-based station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./ClientInstall_x86_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM client configuration utility opens, and displays the Introduction panel.

8 Click on the Next button.

9 Accept the terms of the license agreement in the “Software License Agreement” panel.

10 Click on the Next button.

11 Choose Client Configuration in the “Choose Installation Type” panel.

12 Click on the Next button.

13 Click on the Next button in each subsequent panel until the “Main Server Configuration” panel is displayed.

14 Select the “Enable Secure Communication” parameter.

15 Click on the Next button.

16 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

17 Select the “Start the 5620 SAM Client” parameter.

18 Click on the Done button to close the client configuration utility.

19 The 5620 SAM client GUI opens and connects to the main server, which updates the client configuration. Subsequent client-server communication uses SSL.

Procedure 10-5 To enable SSL on a Windows GUI client

Perform this procedure to enable SSL on a 5620 SAM GUI client that runs on Windows.

Note — To enable or disable SSL on a single-user GUI client or delegate client, you must uninstall the single-user client or client delegate server software, and then select the appropriate SSL option during the client or client delegate server re-installation. A GUI client cannot connect to a main server that has a different SSL configuration, so the main server cannot update the client SSL configuration.

1 Close the client GUI, if it is open, by choosing Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The client GUI closes.

3 Uninstall the client or client delegate server by performing the appropriate procedure in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

4 Navigate to the Windows directory on the 5620 SAM software DVD-ROM.

5 Double-click on the ClientInstall_SAM_9_0_*revision*.exe file

where *revision* is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM client configuration utility opens, and displays the Introduction panel.

6 Click on the Next button.

7 Accept the terms of the license agreement in the “Software License Agreement” panel.

8 Click on the Next button.

9 Choose Client Configuration in the “Choose Installation Type” panel.

10 Click on the Next button.

11 Click on the Next button in each subsequent panel until the “Main Server Configuration” panel is displayed.

12 Select the “Enable Secure Communication” parameter.

13 Click on the Next button.

14 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

15 Select the “Start the 5620 SAM Client” parameter.

16 Click on the Done button to close the 5620 SAM client configuration utility.

17 The 5620 SAM client GUI opens and connects to the main server, which updates the client configuration. Subsequent client-server communication uses SSL.

Procedure 10-6 To enable HTTPS on an OSS client

Perform this procedure to enable an OSS client application to use secure HTTP, or HTTPS, for communicating with a 5620 SAM main server.

1 Ensure that SSL is enabled in the 5620 SAM system, as described in this chapter.

2 Perform the following steps to modify the URL that the OSS application uses to reach the main server.

- **i** Change http: to https:.
- **ii** Change the port value in the URL from 8085 to 8444.

11 — 5620 SAM integration with other Alcatel-Lucent systems

11.1 5620 SAM integration overview

You can configure the 5620 SAM to operate interactively with other Alcatel-Lucent systems. Depending on the nature of the integration, you can use an interface on one system to perform functions on, or retrieve information from, the other system.

For information about 5620 SAM interworking with non-Alcatel-Lucent systems, see the *5620 SAM Integration Guide*.

11.2 5620 SAM and 5650 CPAM integration

When the 5650 CPAM software is enabled on a 5620 SAM system, the 5650 CPAM functions are available from the 5620 SAM main menu. The 5650 CPAM provides real-time control IGP topology capture, inspection, visualization, and troubleshooting. The integration with the 5620 SAM allows the 5650 CPAM to cohesively associate routing information to infrastructure such as network routes, service tunnels, LSPs, edge-to-edge service traffic paths, and OAM tests. See the *5650 CPAM User Guide* for more information.

5650 CPAM and 5620 SAM integration supports the following operational activities:

- **network planning**
  Planning activities are optimized with real-time topology and strong linkages between services and infrastructure layers in the 5620 SAM GUI and 5620 SAM-O OSS interfaces.
- **network operations**
  Real-time topology and multi-layer highlighting allows you to rapidly assess the state of services, tunnels, and routing on the IGP and IP/MPLS maps.
- **network troubleshooting**
  Historical OAM trace, SPF and RSVP path, and checkpoints allow you to rapidly detect and resolve service level issues whose root cause is in the IP or MPLS layers.
- **network restoration**
  Checkpoints and real-time views of IP/MPLS and service and tunnel infrastructure allow you to restore and plan networks.
- **proactive assurance**
  5650 CPAM alarms, network route and tunnel inspection lists, validation functions, checkpoints, and multi-layer views allow you to detect routing faults.

The 5650 CPAM provides a tight eastbound and westbound integration with the 5620 SAM. This integration allows for a real-time view of the network including routing topology and associated configurations whether performed on the GUI, OSS interface, or by CLI. The 5650 CPAM can leverage 5620 SAM redundancy and offer tight navigation between protocol maps and 5620 SAM-managed objects, such as protocol links. In addition, the 5620 SAM GUI supports the management of the 7701 CPAA platform.

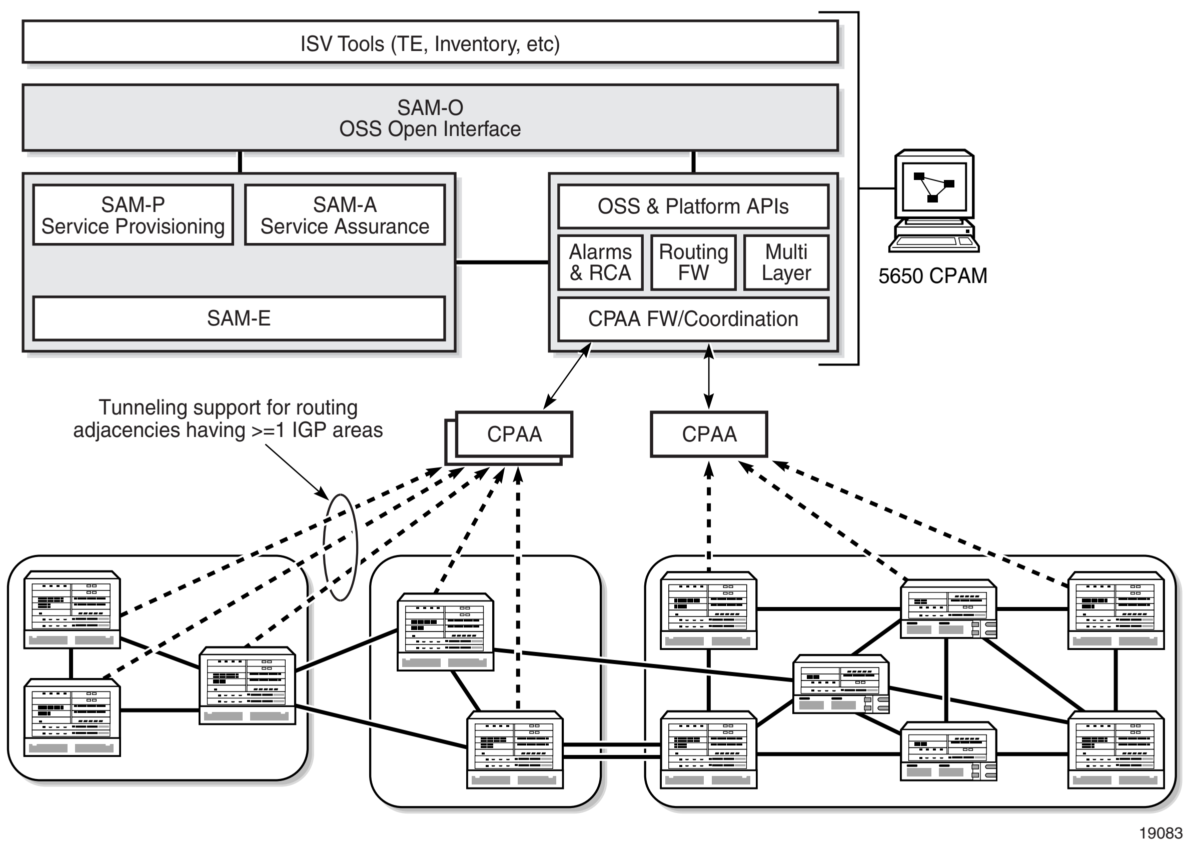
The 5620 SAM-O OSS interface module includes 5650 CPAM packages and methods that provide a smooth integration path for the export of real-time protocol or IP-level topology to advanced OSS applications, such as TE tools.

When the 5650 CPAM and the 5620 SAM share the same database, the 5650 CPAM can access objects managed by 5620 SAM and display them on the 5650 CPAM topology views. Without integration with the 5620 SAM, the following functions are not available:

- service, LSP, multicast, and OAM highlights
- historical LSP active paths
- LDP and RSVP interface display on the MPLS view

Figure 11-1 shows the 5650 CPAM architecture. See the 5650 CPAM documentation suite for information about how to configure application interoperation.

Figure 11-1 5650 CPAM and 5620 SAM integration



There are two main components to the control plane assurance management solution:

- a server component, the 5650 CPAM route controller
- a route analyzer component, the 7701 CPAA

The 5650 CPAM server component contains 7701 CPAA control frameworks, applications, and coordination functions for the distributed 7701 CPAAs and provides the applications that are required to leverage the data provided by the 7701 CPAA platform.

The 5650 CPAM route controller, or server, communicates with several GUI and OSSI clients using the same API as the 5620 SAM. When the 5650 CPAM route controller is integrated with a 5620 SAM, the 5620 SAM and 5650 CPAM versions must be compatible. In addition, the 5650 CPAM route controller can run independently with one or multiple 5620 SAM servers.

The 7701 CPAA is a mountable rack that provides an analysis and distributed computing platform. This platform uses a passive version of the industry-tested and -proven 7750 SR routing code base to guarantee a high degree of interoperability with customer networks. The 7701 CPAA acts as a special-purpose routing element whose role is to passively peer with the network.

The 7701 CPAA is supported by the 5620 SAM as a special-purpose NE.

5650 CPAM deployment

The 5650 CPAM is supported on Solaris platforms only. For system configuration requirements, contact the appropriate Alcatel-Lucent NSM representatives or see the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. System configurations depend on the size of the managed network.

The 5650 CPAM requires a license key to operate. The license key specifies the number of appliances, routers, and GUI clients that the system can support, and the expiry date of the license key.

The 5650 CPAM can be installed by entering the 5650 CPAM license key during the 5620 SAM installation.

If the 5620 SAM is already installed and running, you must enable the 5650 CPAM by adding the appropriate 5650 CPAM license key to the nms-server.xml file. You do not have to re-start the server. You must run the nmsserver.bat or .bash file with the read_config option to activate the 5650 CPAM. If the 5650 CPAM is installed and running without the 5620 SAM, you can enable the 5620 SAM by adding the appropriate 5620 SAM license key to the nms-server.xml file.

The 5650 CPAM works with the 5620 SAM to manage the same network using the same database instance. The 5650 CPAM network may include devices that are not managed by the 5620 SAM.

For example, network A is managed by the 5620 SAM, Release 8.0 and network B is managed by the 5620 SAM, Release 9.0. The 5650 CPAM is connected to both networks. In the integration scenario, the Release 9.0 5620 SAM system and the 5650 CPAM system manage the same network using the same database instance. The network managed by the 5650 CPAM is normally larger than the network managed by the 5620 SAM because it may include several devices that the 5620 SAM does not support.

Database upgrade

The 5620 SAM and the 5650 CPAM share the same database in an integrated deployment.

5650 CPAM uninstallation

You can uninstall the 5650 CPAM from a 5620 SAM/5650 CPAM integration by removing the 5650 CPAM license key from the nms-server.xml file. You must run the nmsserver.bat or .bash file with the read_config option to deactivate the 5650 CPAM.

5650 CPAM menus

Table 11-1 describes the 5650 CPAM menus.

Table 11-1 5650 CPAM menus

Menu item	Description	Dependencies
Tools→Route Analysis	Access all 5650 CPAM management menus	Disabled if the 5650 CPAM license key is not enabled
Application→Flat Maps	View the following flat topology maps: • IGP Topology • OSPF Topology • ISIS Topology • MPLS Topology • Multicast Topology	These flat map options do not appear if the 5650 CPAM license key is not enabled

11.3 5620 SAM and 5620 NM integration

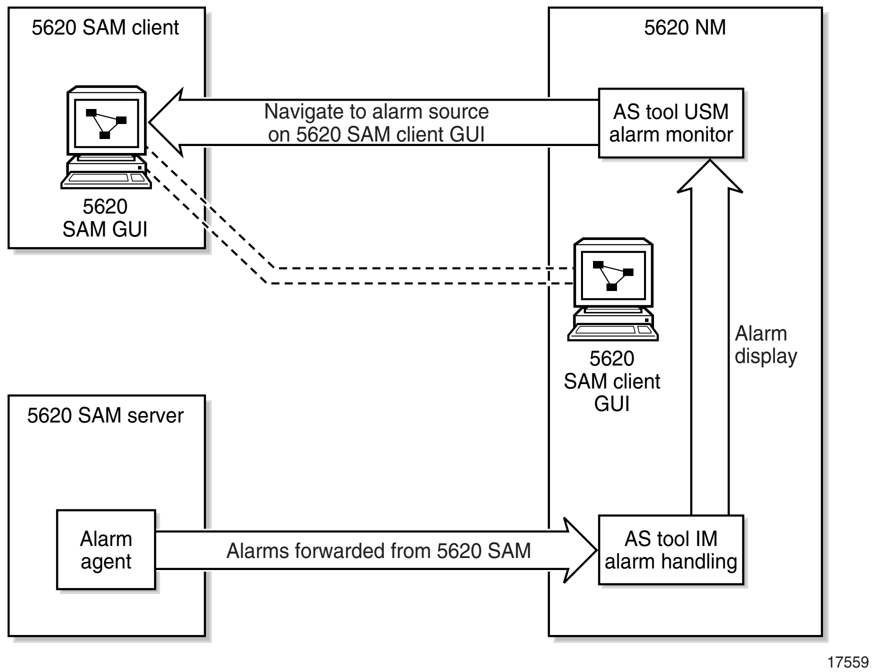
You can integrate the 5620 SAM and 5620 NM, which enables an operator to do the following.

- Navigate the 5620 SAM GUI using a 5620 NM client.
- Forward alarms from the 5620 SAM to the 5620 NM AS tool IM.
- Display 5620 SAM alarms graphically on the 5620 NM AS tool USM.
- Monitor services end-to-end using supported NM integration functions.

Note — Before you can integrate the 5620 SAM and 5620 NM, you must enable navigation from external systems during a 5620 SAM main server installation or upgrade, or enable it after an installation or upgrade using the 5620 SAM server configuration utility. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling navigation from external systems.

Figure 11-2 shows how navigation to the 5620 NM and 5620 NM AS tool for alarm management occurs.

Figure 11-2 Alarm navigation



Before you start

Consider the following before you attempt to integrate the 5620 SAM and 5620 NM:

- The *5620 NM Release Notice* lists the 5620 SAM releases that are compatible with various 5620 NM releases.
- The 5620 NM and 5620 SAM integration software is on the 5620 SAM software DVD-ROM.
- For 5620 SAM GUI navigation using a 5620 NM client, the 5620 SAM client must be installed on the same station that runs the 5620 NM client X-window access application.
- For alarm forwarding, the 5620 SAM and 5620 NM client software can be installed on the same or different stations.
- The platform for the 5620 NM software must meet the minimum requirements in the *5620 Network Manager Installation and Upgrade Guide*.
- You must configure the 5620 SAM to interwork with the 5620 NM software; for example, configure the 5620 SAM server to forward alarms and configure the 5620 SAM client to allow navigation from external systems.

5620 SAM client GUI startup and navigation restrictions

The following restrictions apply to 5620 SAM client GUI navigation using a 5620 NM client.

- When the client GUI is starting, 5620 NM navigation requests are blocked.
- A 5620 SAM client accepts navigation requests after the client GUI user logs in.

- Each navigation request is submitted only after a login timeout expires. This timeout helps to decrease the number of requests that are sent when a user submits and then immediately cancels a request.
- A 5620 SAM client delegate server acts as a single 5620 SAM client instance; you cannot configure a client delegate server to integrate with more than one 5620 NM client.
- The following navigation rules apply when multiple client GUIs are running.
  - A navigation request is cancelled when the client GUI is shut down.
  - All navigation requests are handled by the first registered client GUI.
  - If no client GUI is registered, a 5620 SAM server starts a new client GUI when it receives a navigation request.
  - If the currently registered 5620 SAM client GUI shuts down, another registered client GUI handles the navigation requests.

11.4 Workflow for 5620 SAM and 5620 NM integration

1. Ensure that the appropriate 5620 SAM integration software is installed and appropriately configured on the 5620 NM. See Procedure 11-1 for more information.
2. Configure the 5620 SAM client and server to support GUI navigation. See Procedure 11-2 for more information.
3. Start the 5620 SAM GUI. See section 3.4 for more information.
4. Start the 5620 NM client GUI. See Procedure 11-3 for more information.
5. Perform the required network management function using the appropriate GUI, as described in section 11.3.

11.5 5620 SAM and 5620 NM integration procedures

The following procedures describe how to configure 5620 SAM and 5620 NM integration.

Procedure 11-1 To configure 5620 SAM and 5620 NM GUI integration

Perform this procedure to enable the use of a 5620 SAM client GUI through a 5620 NM client GUI.

1. Include the required 5620 SAM integration package in the 5620 NM installation. Consult the 5620 NM documentation for integration software installation and configuration information.
2. If required, configure the 5620 SAM server to forward alarms to the 5620 NM, as described in section 11.3.
3. If navigation from external systems is not currently enabled on each 5620 SAM main server, perform Procedure 11-2.

4 Install a 5620 SAM GUI client on a station that displays the 5620 NM client GUI. This is typically a station that runs an X-Window terminal emulator, but it can also be the 5620 NM database networkstation or the 5620 NM operator server networkstation, if a client GUI is locally displayed.

5 Perform one of the following on the station where the 5620 SAM client is installed.

a On a Solaris station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically /opt/5620sam/client/nms/config

b On a Windows station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically C:\5620sam\client\nms\config

6 Perform the following steps to ensure that anti-aliasing is disabled.

i Search for the following XML tag that marks the beginning of the topologyMaps section:

```
<topologyMaps
```

ii Edit the antiAliasActive entry in the topologyMaps section to read “false” as shown below.

```
<topologyMaps
     iconReductionThreshold="40"
     labelHideThreshold="35"
        snapToGridInterval="25"
        antiAliasActive="false"
     />
```

7 Open a console window on the station.

8 Perform one of the following to run the navigator proxy script and start the client software.

a On a Solaris station, perform the following steps.

i Enter the following at the CLI prompt:

\# **cd *path***

where *path* is the 5620 SAM client binary directory, typically /opt/5620sam/client/nms/bin

ii Enter the following:

```
# ./install_navigation_daemon.bash
```

iii Enter the following:

```
# ./nmsclient.bash
```

b On a Windows station, perform the following steps.

i Enter the following at the CLI prompt:

cd *path*

where *path* is the 5620 SAM client binary directory, typically C:\5620sam\client\nms\bin

ii Enter the following:

```
install_navigation_service.bat
```

iii Enter the following:

```
nmsclient.bat
```

The GUI client starts.

9 Use the 5620 SAM client GUI to create a 5620 NM user account that has a non-administrative privilege level with the appropriate scope of command role applied. See chapter 9 for more information about configuring user accounts and how to apply a scope of command role.

10 Copy /opt/5620sam/server/nms/lib/common/generated/nms_common_core.jar from a 5620 SAM main server to the opt/netmgt/jnm/samjms/lib directory on the 5620 NM database networkstation.

11 Copy the following files from the /integration/5620NM/client/samadaptor directory on the 5620 SAM integration DVD-ROM to the /opt/netmgt/samadaptor/lib directory on the 5620 NM database networkstation:

- jbasiccomp.jar
- jnavapi.jar
- navrmi.jar
- samAdaptor.jar

12 Open the X-Window terminal emulator on the station that has the newly installed 5620 SAM client.

13 Log in to the 5620 NM operator server networkstation as a user with administrative privileges.

14 Open a console window on the 5620 NM operator server networkstation.

15 Start the 5620 NM client. The 5620 NM client GUI is displayed on the local station, and the 5620 SAM client GUI is available as a 5620 NM main menu item.

16 Use the 5620 SAM client account created in step 9 to perform the required interworking functions, as described in described in section 11.3, and the *5620 Network Manager User Guide*.

Procedure 11-2 To enable navigation from external systems on a 5620 SAM main server

1 Log in to the main server station as the root user.

2 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

3 Open a console window.

4 Navigate to the DVD-ROM drive.

5 If the main server is installed on a SPARC station, enter the following to open the configuration utility:

```
# Solaris/ServerInstall_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

6 If the main server is installed on an x86-based station, enter the following to open the configuration utility:

```
# Solarisx86/ServerInstall_SAM_9_0_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

7 Click on the Next button.

8 Accept the terms of the license agreement in the “Software License Agreement” panel.

9 Click on the Next button.

10 Choose Main Server Configuration in the “Choose Installation Type” panel.

11 Click on the Next button.

12 Click on the Next button in each subsequent panel until the “Navigation from External Systems” panel is displayed.

13 Select the “Enable Navigation from External Systems” parameter.

14 Configure the “TCP port for accepting GUI navigation requests” parameter.

15 Click on the Next button.

16 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

17 Click on the Done button to close the server configuration utility.

18 Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

19 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

20 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration changes into effect.

Procedure 11-3 To start the 5620 NM GUI

1 Log in to the 5620 SAM single-user client or client delegate station

2 Start the X-terminal software.

3 Use the X-terminal software to start the 5620 NM GUI on the Solaris station that has the 5620 NM Operator Position installed.

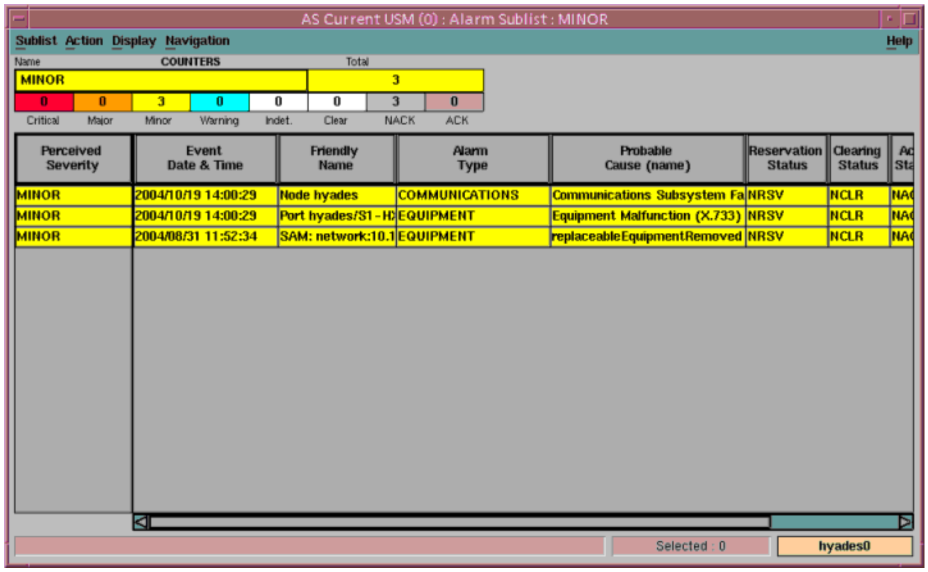
Procedure 11-4 To navigate from the 5620 NM AS tool USM to the 5620 SAM client GUI

See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using alarms.

1 Choose a counter summary window or alarm sublist from the AS tool USM.

2 Choose a sublist or an alarm in a sublist. 5620 SAM alarms are preceded by SAM in the Friendly Name field of the alarm sublist, as shown in Figure 11-3.

Figure 11-3 5620 SAM alarm in the AS tool USM



3 From the 5620 NM AS tool USM menu, choose Navigation→External Equipment→Show Equipment to navigate to the property form that lists the alarm on the 5620 SAM client GUI. The appropriate form is displayed. If the 5620 SAM client GUI is running, a new object properties form is displayed.

4 If the client GUI is not running, perform the following steps.

  i Open the 5620 SAM client GUI.

  ii View the object property form that is displayed on the 5620 NM client GUI.

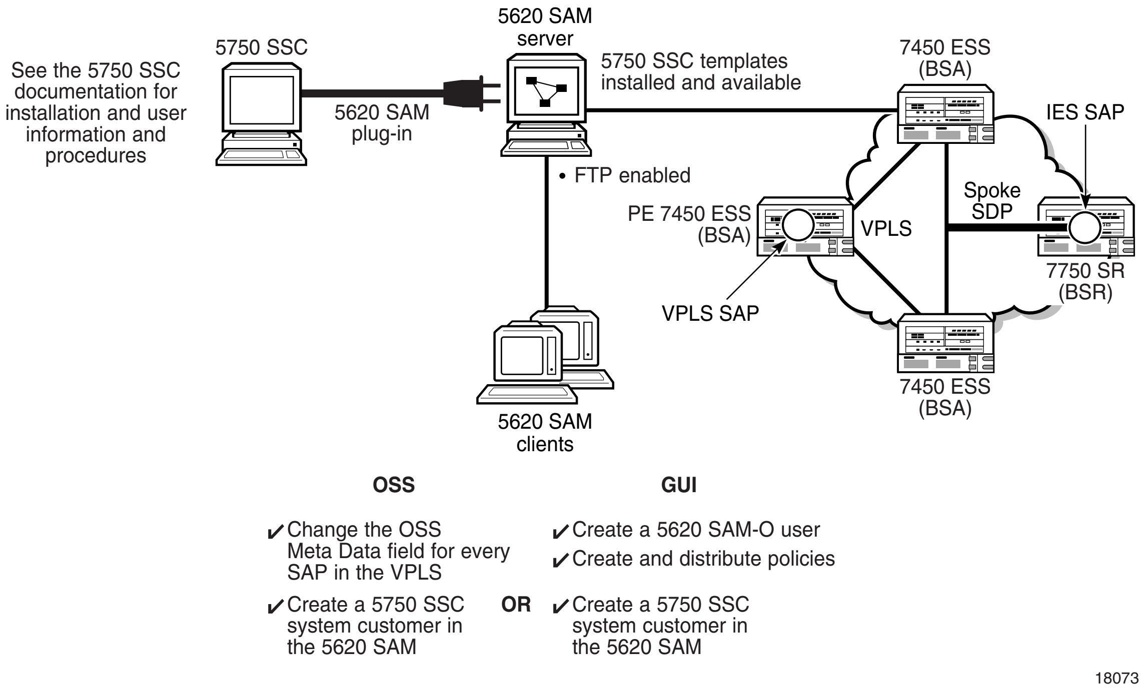
5 After the alarm issue is resolved, clear the alarm using the 5620 SAM client GUI. Alarm status changes are shown in the 5620 NM AS tool USM.

11.6 5620 SAM and 5750 SSC integration

The 5620 SAM can be configured to interoperate with the 5750 Subscriber Services Controller. The 5750 SSC provides centralized control of subscriber access services for triple play service delivery; for example, DHCP to identify subscribers and trigger service configuration.

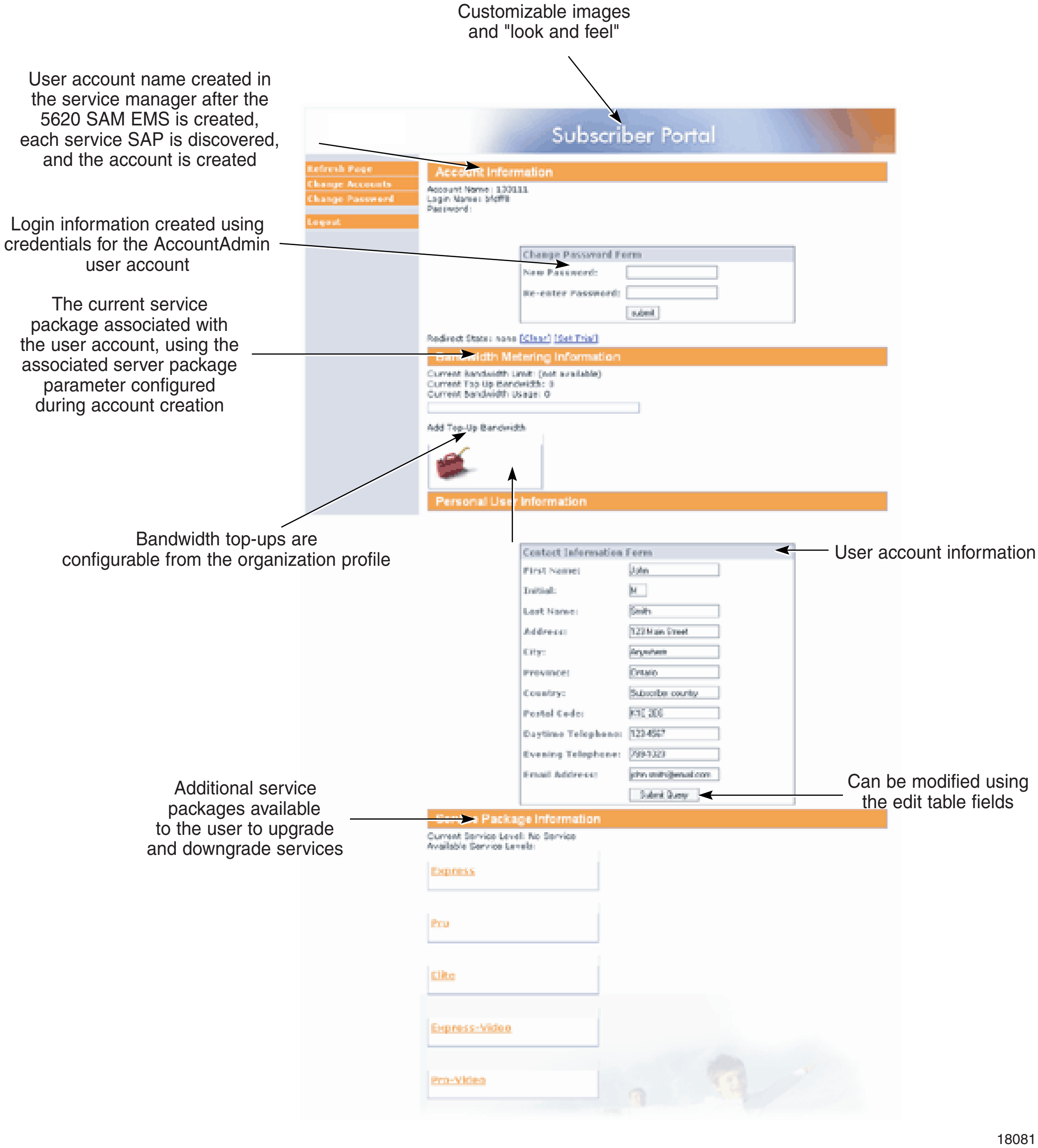
Figure 11-1 shows the integration requirements for the 5620 SAM and the 5750 SSC. See the 5750 SSC documentation suite for information about how to configure application interoperation.

Figure 11-4 5750 SSC and 5620 SAM integration



You use the 5750 SSC Service Manager to create and manage subscriber services, including user account information and QoS levels. The 5750 SSC user accounts represent the residential subscribers of triple play services. The information configured in the 5750 SSC Service Manager is used to build the subscriber web portal for user self-management. Figure 11-5 shows a subscriber web portal and how the component pieces are assembled from 5750 SSC subscriber management configurations.

Figure 11-5 Subscriber web portal



11.7 5620 SAM and 5780 DSC integration

The 5780 DSC is treated as a device that is managed by the 5620 SAM, rather than an external system that requires integration with the 5620 SAM. The 5620 SAM allows you to view the properties for the equipment, instance, Diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC is represented in the 5620 SAM equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances 5620 SAM main menu option.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 5780 DSC management. The following documents describe 5620 SAM management and configuration of the 5780 DSC:

- *5620 SAM LTE ePC User Guide*—Describes 5780 DSC discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes the 5780 DSC parameters that are represented in the 5620 SAM schema, and parameters on LTE and LTE service forms in the 5620 SAM GUI

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

11.8 5620 SAM and the 5620 SAM Supervision Module

The 5620 SAM Supervision Module is a web-based application that provides a summarized, at-a-glance view of NEs and objects in the 5620 SAM network. You can use the supervision module to group and monitor network resources that are natively managed by the 5620 SAM or by a subtending network management system that is interfaced with the 5620 SAM for supervision purposes.

You can access the 5620 SAM Supervision Module by choosing Application→Supervision Portal from the 5620 SAM main menu. The supervision module launches if you have specified a web browser in the user preferences. See the *5620 SAM Supervision Module User Guide* for more information.

Table 11-2 describes the menu objects.

Table 11-2 5620 SAM Supervision Module menu objects

Menu object	Description
Application→Supervision Portal	Launches the 5620 SAM Supervision Module web portal
Administration→Supervision Settings	Allows you to configure KPI timers and create the following supervision module objects: • supervision groups • summary views

Device management

28 — Object life cycle

29 — Auto-provision

12 — Device support

12.1 Device support overview

The 5620 SAM can manage the following Alcatel-Lucent devices:

- 1830 PSS-1
- 1830 PSS-16
- 1830 PSS-32
- 1830 PSS-4
- 5780 DSC
- 7210 SAS-D 6F 4T
- 7210 SAS-D 6F 4T ETR
- 7210 SAS-E
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 MG
- 7750 SR
- 7750 SR-c4
- 7750 SR-c12
- 9471 MME
- 9500 MPR
- eNodeB
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6900
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E
- OS 10K

The 5620 SAM can also manage Telco devices, and provides limited management support for other third-party devices, which are called generic NEs.

For core-network devices such as the 7450 ESS, 7710 SR, and 7750 SR, the 5620 SAM supports the current software release and the three immediately previous major releases. For example, a Release 9.0 5620 SAM system can manage a 7750 SR at Release 9.0, 8.0, 7.0, 6.1, or 6.0. Older device releases are not supported.

For devices other than core-network devices, the 5620 SAM release support varies. See the *5620 SAM Network Element Compatibility Guide* for specific device support information.

Caution — When a device introduces a maintenance release, you must ensure that your 5620 SAM software supports the new device release before you upgrade the device to the new release. You may need to upgrade the 5620 SAM to support the new device release. See the current *5620 SAM Network Element Compatibility Guide* for more information.

The 5620 SAM GUI displays a device feature or function only if the device supports the feature or function. The 5620 SAM user documentation describes the major variations in support, including device-specific procedures for specific implementations, but does not describe the following minor GUI variations for different devices:

- partial support for the parameter list on a form
- partial support for the buttons and tabs on a form

The following documents describe 5620 SAM support for specific device releases:

- *5620 SAM Network Element Compatibility Guide*—lists the device releases and functions that the 5620 SAM supports
- *5620 SAM Parameter Guide*—lists and describes the supported parameters; includes device-specific variations in parameter defaults and ranges

See the device user documentation for information about device functions, parameters, and CLI commands that are outside the scope of the 5620 SAM documentation. Contact Alcatel-Lucent technical support for specific network or facility considerations.

Workflows

The *5620 SAM User Guide* describes the management of many devices, however 5620 SAM management of some devices, for example, optical and LTE devices, is described in other guides. Each device-specific section in this chapter contains one of the following:

- a workflow for device discovery and management, if within the scope of the *5620 SAM User Guide*
- a reference to the guide that describes 5620 SAM management of the device

A device-specific workflow in this chapter lists the high-level steps required to do the following:

- commission, configure, and manage the device
- create and manage customer services on the device

You can use a device workflow to determine which device functions you require, and then systematically enable and configure the functions.

12.2 Workflow for general device management

The following workflow lists the initial high-level 5620 SAM management steps that are common to all devices. See the other workflows in this chapter as required for device-specific workflow steps.

1. View information about specific 5620 SAM device support. See this chapter for more information.

2. View the 5620 SAM license for information about the consumed and remaining device quantities and update if required. See chapter 6 for more information.

3. Change the license key in a standalone or redundant 5620 SAM system. See chapter 6 for more information.

4. Commission the device for 5620 SAM management. See chapter 13 for more information.

5. Configure in-band and out-of-band management, as required. See chapter 13 for more information.

6 Configure a polling policy. See chapter 13 for more information.

7 As required, change the system name of the device. This may be required, for example, because of network reconfiguration, or the management of a new device that has the same name as a currently managed device. See chapter 6 for more information.

12.3 1830 PSS support

The 1830 Photonic Service Switch product family provides advanced CWDM, DWDM, and OTN capabilities. It provides increased network flexibility and operational automation using zero-touch, transparent photonic networking. The 5620 SAM supports the following 1830 PSS devices:

- 1830 PSS-1 - edge aggregation device; the supported variants are the following:
  - 1830 PSS-1 AHP amplifier
  - 1830 PSS-1 GBE edge device
  - 1830 PSS-1 MD4H edge device
- 1830 PSS-16 - end office device
- 1830 PSS-32 - central office device
- 1830 PSS-4 - edge device

The *5620 SAM User Guide* and other non-optical documents in the 5620 SAM documentation suite do not describe 1830 PSS management. The following documents describe 5620 SAM management and configuration of the 1830 PSS:

- *5620 SAM Optical User Guide*—Describes 1830 PSS discovery, configuration, and management using the 5620 SAM
- *5620 SAM Optical Parameter Reference*—Provides a list of all optical device parameters that the 5620 SAM supports

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

12.4 5780 DSC support

The 5620 SAM allows you to view the properties for the equipment, instance, Diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC is represented in the 5620 SAM equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances 5620 SAM main menu option.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 5780 DSC management. The following documents describe 5620 SAM management and configuration of the 5780 DSC:

- *5620 SAM LTE ePC User Guide*—Describes 5780 DSC discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes the 5780 DSC parameters that are represented in the 5620 SAM schema, and parameters on LTE and LTE service forms in the 5620 SAM GUI

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

12.5 7210 SAS support

This section describes the 5620 SAM support for Alcatel-Lucent 7210 SAS devices.

7210 SAS-D support

The 7210 SAS-D is an intelligent Ethernet edge-demarcation device that extends enhanced Carrier Ethernet VPN service delivery to the CE. The license for a 7210 SAS-D is based on the chassis type. The 5620 SAM supports the following chassis types:

- 7210 SAS-D 6F 4T
- 7210 SAS-D 6F 4T ETR

5620 SAM support for the 7210 SAS-D includes the following:

- access and uplink modes for Ethernet ports
- alarm management
- configuration backups and restores
- egress port rate limiting
- frame-based accounting
- hardware:
    - 4 x 10/100/100BaseT MDA
    - 6 x 100/1000 SFP MDA
- H-Metering
- LAGs
- LLF
- OAM diagnostic tests:
    - CFM and EFM
    - DNS ping
    - ICMP ping
    - ICMP trace

- QoS policies:
    - 7210 Access Egress
    - 7210 Network
    - 7210 Network Queue
    - 7210 Port Access Ingress
    - 7210 Port Scheduler
    - 7210 Slope
- services:
    - IES, using in-ban d management only
    - VLL Epipe
    - VPLS
- software upgrades
- statistics collection

Note — The 5620 SAM supports only access mode for 7210 SAS-D 6F 4T ETR ports.

7210 SAS-E support

The 7210 SAS-E is a Carrier Ethernet CE device that is typically owned and managed by a customer. Using software based on the 7750 SR OS and managed by the 5620 SAM, the 7210 SAS-E extends Carrier Ethernet VPN services to the CE. The 7210 SAS-E can also be deployed as an aggregation device for smaller sites.

5620 SAM support for the 7210 SAS-E includes the following:

- access and uplink modes for Ethernet ports
- alarm management
- configuration backups and restores
- egress port rate limiting
- frame-based accounting
- hardware:
    - integrated IOM and Ethernet ports
    - 12 x 100/1000 SFP Ethernet ports; and copper SFPs
    - 12 x 10/100/1000 TX Ethernet ports
- in-band and out-of-band management; out-of-band management is supported only on Release 2.0 R2 or later
- G.8032 Ethernet Ring Protection
- LAGs
- LLDP
- OAM diagnostic tests:
    - CFM and EFM
    - DNS ping
    - ICMP ping
    - ICMP trace

- QoS policies:
    - 7210 Access Egress
    - 7210 Access Ingress
    - 7210 Network
    - 7210 Network Queue
    - 7210 Port Access Egress
    - 7210 Port Scheduler
    - 7210 Queue Management
    - 7210 Remarking
    - 7210 Slope
- services:
    - IES, using in-ban d management only
    - VLL Epipe
    - VPLS
- software upgrades
- static routes for in-band management
- statistics collection

7210 SAS-E daughter cards

The 7210 SAS-E supports an integrated 2 x 12-Gig IOM card on a single chassis. The equipment navigation tree displays a card slot with one daughter card that contains 12 x 100/1000 Ethernet SFP ports and 12 x 10/100/1000 Ethernet ports.

7210 SAS-M and 7210 SAS-X support

The 7210 SAS-M is a CE device that provides MPLS-enabled metropolitan and WAN Carrier Ethernet service delivery, Ethernet-based mobile backhaul, and residential service access.

The 7210 SAS-X is an MPLS-enabled Ethernet aggregation device for small and medium-sized networks that provides business, mobile backhaul, and residential services. It is similar to the 7210 SAS-M, but has 10Gb/s uplink ports, enhanced traffic management, greater scalability, and hierarchical QoS functions.

The 5620 SAM supports the following 7210 SAS-M and 7210 SAS-X chassis types:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP

Note — If you use the CLI or BOF to change the mode of a 7210 SAS-M from Access Uplink to Network, or from Network to Access Uplink, you must unmanage and remanage the device. The mode is shown on the Uplink Mode tab of the shelf properties form.

5620 SAM support for the 7210 SAS-M and 7210 SAS-X includes the following:

- alarm management
- configuration backups and restores
- egress port rate limiting
- frame-based accounting
- G.8032 Ethernet Ring Protection, 7210 SAS-X 24F 2XFP 3.0R2 and later only
- hardware:
    - 2-Port Gig Ethernet MDA with SyncE, 7210 SAS-M only
    - 2x10GigE XFP MDA, 7210 SAS-M in L2 access uplink mode only
    - 24 x 10/100/1000 Ethernet SFP ports
    - 4 x Channelized DS1/T1 CES MDA; does not support uplink mode
    - two 10 GigE ports, only on 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP
- H-metering
- in-band and out-of-band management; out-of-band management is supported only on the 7210 SAS-M, Release 2.0 R2 or later
- IP/MPLS:
    - RSVP
    - T-LDP
- LLDP
- OAM diagnostic tests:
    - CFM and EFM
CPE Ping
DNS Trace
ICMP Ping
ICMP Trace
LSP Ping
LSP Trace
MAC Ping
MAC Populate
MAC Purge
MAC Trace
MTU Ping
SVC Ping
Tunnel Ping
VCCV Ping
- policy audits
- QoS policies:
    - 7210 Access Ingress
    - 7210 Access Egress
    - 7210 Network
    - 7210 Network Queue
    - 7210 Port Access Egress
    - 7210 Port Scheduler
    - 7210 Queue Management
    - 7210 Remarking
    - 7210 Slope

- routing:
  - ISIS
  - OSPF
  - static routes
- security management
- services:
  - CESoP Cpipe for CES MDA, 7210 SAS-M only
  - IES, using in-ban d management only
  - VLL Epipe
  - VLL Cpipe, 7210 SAS-M only
  - VPLS (ELAN)
  - spoke SDP bindings
- software upgrades
- statistics collection

12.6 Workflow to manage 7210 SAS devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7210 SAS NEs and services. This workflow assumes that the physical devices have been installed.The management functions are supplemental to the general management functions described in section 12.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 13 for more information. Configure polling policies as described in Procedure 13-12.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

4 As required, manage and configure equipment; see chapter 16 for more information about equipment management and configuration. Additionally, configure the following, as required:

a split horizon groups as described in Procedure 20-16

b LAGs as described in Procedures 18-13 and 18-14

c frame-based accounting as described in Procedure 17-11

d dry contact sensors as described in Procedure 19-2

e channelized TDM ports as described in Procedure 20-14

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21 for more information.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

7 Create equipment inventories of managed devices; see chapter 22 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs; see chapter 24 for more information
- **b** threshold-crossing alarms; see chapter 26 for more information
- **c** bulk configuration changes; see chapter 27 for more information
- **d** object life cycle management; see chapter 28 for more information
- **e** automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 31 for more information.
- **b** MPLS and LSPs; see chapter 32 for more information.
- **c** service tunnels to carry service traffic; see chapter 33 for more information.
- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** 5620 SAM alarm policies; see chapter 37 for more information
- **g** OAM diagnostic tests; see chapter 38 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information
- **c** MC peer groups; see chapter 41 for more information
- **d** MC endpoint groups; see chapter 42 for more information
- **e** MC LAG groups; see chapter 43 for more information
- **f** MC synchronization groups; see chapter 44 for more information
- **g** MC ring groups; see chapter 45 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 47 and Procedures 47-2, 47-4, 47-5, 47-7, 47-9, 47-11, 47-13, 47-19, and 47-25 for more information
- **b** multicast policies; see chapter 49 for more information

- **c** time of day policies; see chapter 50 for more information
- **d** VRRP policies; see chapter 51 for more information
- **e** auto tunnels policies; see chapter 52 for more information
- **f** 802.1x policies; see chapter 54 for more information
- **g** PBB MRP policies; see chapter 55 for more information
- **h** connection profile policies; see chapter 57 for more information
- **i** service PW template policies; see chapter 58 for more information
- **j** residential subscriber policies; see chapter 59 for more information
- **k** remote network monitoring policies; see chapter 60 for more information
- **l** size constraint policies; see chapter 61 for more information
- **m** NAT policies; see chapter 62 for more information
- **n** format and range policies; see chapter 63 for more information

12 Configure services and related functions; see chapters 64 and 65 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLL Epipe services as described in Procedure 70-2
- **e** VLL Apipe, Cpipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **f** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain as described in Procedure 71-2. See chapter 71 for more information.
- **g** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **h** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **i** composite services to connect various types of services; see chapter 76 for more information
- **j** 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information

k OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information

l Ethernet Connectivity Fault Management; see chapter 80 for more information

m RCA audit; see chapter 81 for more information

12.7 7250 SAS and Telco device support

The Alcatel-Lucent 7250 SAS devices and Telco devices support Ethernet and service-aware Ethernet aggregation across IP/MPLS networks. Typically, these devices are connected in rings or trees to 7450 ESS devices to distribute L2 VPN or BTV services in VLANs.

The 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA can backhaul TDM lines through the core network using two 4-port CES modules. A 5620 SAM operator configures a CES module to receive E1 or T1 transmission, and then creates an interface on a logical port in the CES module to enable circuit emulation with dot1q encapsulation.

The 7250 SAS-ES and 7250 SAS-ESA support all 7250 SAS functions, and have two additional GigE uplink ports that support the following:

- hierarchical QoS
- RSVP-TE and FRR
- MPLS LSR
- VPLS

The 7250 SAS-ESA also supports dry contact sensors. Four dry contact sensor inputs are available in a connector on the back panel of the 7250 SAS-ESA. The sensor inputs can be used to monitor the status of external equipment such as doors, power modules, fans, and batteries. When a sensor input detects a change in the state of a dry contact, the 7250 SAS-ESA sends an SNMP trap to the 5620 SAM. Depending on how the sensor inputs are configured, a change in the state of a dry contact can raise or clear an alarm condition.

The 5620 SAM provides element and network management functions for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices using the CLI and SNMP. When a function is not supported by the device, the function cannot be selected from the GUI or does not appear on the GUI.

12.8 Workflow to manage 7250 SAS and Telco devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 12.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 13 for more information. Additionally, configure the following:

- **a** commissioning as described in Procedure 13-3
- **b** polling policies as described in Procedure 13-11

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

4 As required, manage and configure equipment; see chapter 16 for more information about equipment management and configuration. Additionally, configure the following, as required:

- **a** uplink ports as network ports as described in Procedure 20-18
- **b** dry contact sensors as described in Procedure 19-2
- **c** circuit emulation as described in Procedures 17-21, 17-22, 17-23, 17-24, and 17-25

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

7 Create equipment inventories of managed devices; see chapter 22 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs; see chapter 24 for more information
- **b** threshold-crossing alarms; see chapter 26 for more information
- **c** bulk configuration changes; see chapter 27 for more information
- **d** object life cycle management; see chapter 28 for more information
- **e** automatic provisioning; see chapter 29 for more information

9 As required, configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. Configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 31 for more information. Additionally, configure bridging as described in Procedure 31-53.
- **b** MPLS and LSPs; see chapter 32 for more information. Additionally, configure LSPs as described in Procedures 32-10, 32-11, and 32-12.
- **c** service tunnels to carry service traffic; see chapter 33 for more information
- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** 5620 SAM alarm policies; see chapter 37 for more information
- **g** OAM diagnostic tests; see chapter 38 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information
- **c** MC peer groups; see chapter 41 for more information
- **d** MC endpoint groups; see chapter 42 for more information
- **e** MC LAG groups; see chapter 43 for more information
- **f** MC synchronization groups; see chapter 44 for more information
- **g** MC ring groups; see chapter 45 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies as described in Procedure 47-35. See chapter 47 for more information.
- **b** filter policies as described in Procedures 48-4, 48-5, 48-6, and 48-7. See chapter 48 for more information.
- **c** multicast policies; see chapter 49 for more information
- **d** VRRP policies; see chapter 51 for more information
- **e** auto tunnels policies; see chapter 52 for more information
- **f** 802.1x policies; see chapter 54 for more information
- **g** PBB MRP policies; see chapter 55 for more information
- **h** AOS Ethernet service policies; see chapter 56 for more information
- **i** connection profile policies; see chapter 57 for more information

- **j** service PW template policies; see chapter 58 for more information
- **k** residential subscriber policies; see chapter 59 for more information
- **l** remote network monitoring policies; see chapter 60 for more information
- **m** size constraint policies; see chapter 61 for more information
- **n** NAT policies; see chapter 62 for more information
- **o** format and range policies; see chapter 63 for more information

12 Configure services and related functions; see chapters 64 and 65 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLAN services for subscribers; see chapter 69 for more information
- **e** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **f** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **g** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **h** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **i** composite services to connect various types of services; see chapter 76 for more information
- **j** 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information
- **k** OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information
- **l** Ethernet Connectivity Fault Management; see chapter 80 for more information
- **m** RCA audit; see chapter 81 for more information

12.9 7450 ESS support

The Alcatel-Lucent 7450 ESS sets a new market standard for enabling the delivery of profitable Ethernet business services in metro, national and international network environments. It also provides high density service-aware Ethernet aggregation for consumer triple-play services over IP/MPLS-based networks. The Alcatel-Lucent 7450 ESS is purpose-built for the service provider market, with an architecture that supports a wide range of interfaces and offers unmatched density and performance. The 7450 ESS allows service providers to offer new, revenue-generating services for both the consumer and business markets.

In order to determine which network ports are eligible to transport traffic of individual SDPs, the Network Domain feature has been introduced. This information is used for the SAP-ingress queue allocation algorithm applied to VPLS SAPs. See chapter 30 for more information.

12.10 Workflow to manage 7450 ESS devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7450 ESS NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 12.2.

1. Determine configuration requirements for the installed device; see this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2. Commission the device for 5620 SAM management; see chapter 13 for more information. Configure polling policies as described in Procedure 13-10.

3. Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

4. As required, manage and configure equipment; see chapter 16 for more information about equipment management and configuration. Additionally, configure the following:

    a. mixed mode as described in Procedure 19-4

    b. IEEE 1588 PTP clock as described in Procedures 19-10 and 19-11

5. Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21.

6. If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

7. Create equipment inventories of managed devices; see chapter 22 for more information.

8 As required, perform additional device management functions such as the following:

  a TCP enhanced authentication between NEs; see chapter 24 for more information

  b card migration; see chapter 25 for more information

  c threshold-crossing alarms; see chapter 26 for more information

  d bulk configuration changes; see chapter 27 for more information

  e object life cycle management; see chapter 28 for more information

  f automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

  a NE protocols; see chapter 31 for more information.

  b MPLS and LSPs; see chapter 32 for more information.

  c service tunnels to carry service traffic; see chapter 33 for more information.

  d Lawful Intercept; see chapter 34 for more information

  e IPsec; see chapter 35 for more information

  f ISA-Video; see chapter 36 for more information

  g 5620 SAM alarm policies; see chapter 37 for more information.

  h OAM diagnostic tests; see chapter 38 for more information.

10 As required, configure redundancy in the managed network using functions such as the following:

  a VRRP; see chapter 39 for more information

  b APS; see chapter 40 for more information

  c MC peer groups; see chapter 41 for more information

  d MC endpoint groups; see chapter 42 for more information

  e MC LAG groups; see chapter 43 for more information

  f MC synchronization groups; see chapter 44 for more information

  g MC ring groups; see chapter 45 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

  a QoS policies; see chapter 47 for more information

  b filter policies; see chapter 48 for more information

- **c** multicast policies; see chapter 49 for more information
- **d** time of day policies; see chapter 50 for more information
- **e** VRRP policies; see chapter 51 for more information
- **f** auto tunnels policies; see chapter 52 for more information
- **g** RADIUS-based accounting policies; see chapter 53 for more information
- **h** 802.1x policies; see chapter 54 for more information
- **i** PBB MRP policies; see chapter 55 for more information
- **j** connection profile policies; see chapter 57 for more information
- **k** service PW template policies; see chapter 58 for more information
- **l** residential subscriber policies; see chapter 59 for more information
- **m** remote network monitoring policies; see chapter 60 for more information
- **n** size constraint policies; see chapter 61 for more information
- **o** NAT policies; see chapter 62 for more information
- **p** format and range policies; see chapter 63 for more information

12 Configure services and related functions; see chapters 64 and 65 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **h** VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 74 for more information
- **i** composite services to connect various types of services; see chapter 76 for more information

j Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 77 for more information

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information

m Ethernet Connectivity Fault Management; see chapter 80 for more information

n RCA audit; see chapter 81 for more information

12.11 7705 SAR support

The Alcatel-Lucent 7705 SAR is an IP/MPLS aggregation and mobile backhaul router for the mobile RAN. Located at cell sites, the 7705 SAR uses PW over MPLS to aggregate mobile 2G and 3G traffic that it backhauls to the core network. The 7705 SAR supports ATM, TDM, and Ethernet.

7705 SAR auxiliary alarm daughter cards

The 7705 SAR supports an auxiliary alarm daughter card. This is a unique card that interfaces with real-time systems. The following inputs and outputs are available:

- 24 digital inputs that can connect to dry contacts of security sensors, HVAC systems, and telecom systems
- Two analog inputs for monitoring battery voltage; each supports a range of 0 to 75V and has configurable thresholds for alarms and events on each port
- Eight dry-contact relay outputs that interface to external audible, visual, or telecom equipment using NO or NC contact pins

The inputs and outputs are listed on the Ports tab of the daughter card slot properties form, in the same manner as ports on a data-plane daughter card. Each input or output has configurable parameters. The name specified for each input or output must be unique within the device.

7705 SAR six-port E&M daughter cards

The 7705 SAR supports a six-port E&M daughter card. The configuration of ports and channels on this daughter card is similar to the 16-port DS1/E1 ASAP daughter card. You create a channel under each port, and a channel group under each channel.

The following configuration restrictions and limitations apply to ports and channels on the six port E&M daughter card:

- A port can have only one channel.
- A channel can have only one channel group.

- A channel group must be in Access mode and use CEM encapsulation.
- A channel group MTU is not configurable.

Only CESoPSN Cpipe SAPs can be created on the daughter card.

7705 SAR 12-port SDI card

The 7705 SAR-8/18 supports a 12-port Serial Data Interface card. The SDI card includes four connectors, each of which supports three ports. Each port in a three-port connector must be configured to work on the same interface type. V.35 and X.21 interfaces support FR, CEM, and IPCP encapsulation. The ports operate in access mode and can be configured to work with the following interfaces:

- RS232
- V.35
- X.21

7705 SAR Power Injector card

The 7705 SAR-8/18 supports a Power Injector card to deliver power and data to an MPT radio. Up to four Power Injector cards can be installed on the 7705 SAR-8, and up to eight Power Injector cards can be installed on the 7705 SAR-18.

7705 SAR Optical Add/Drop Mux cards

The 7705 SAR-8/18 supports an Optical Add/Drop Mux (OADM) card in 1, 2, 4, and 8-colour variants. These cards increase bandwidth in a fiber network.

7705 SAR 10-port 1GigE/1-port 10GigE X-Adapter card

The 7705 SAR-18 supports a 10-gigabit Ethernet XMDA which can be configured for ten 1-gigabit ports or one 10-gigabit port.

7705 SAR-F daughter cards

The 7705 SAR-F integrates eight-port Ethernet v3 and 16-port DS1/E1 v2 ASAP MDA functions in one chassis. When the 5620 SAM discovers a 7705 SAR-F, the integrated MDAs are automatically configured and displayed in the equipment tree.

7705 SAR-M daughter cards

The 7705 SAR-M variants are equipped with an integrated 7-port Ethernet card. Depending on the variant, a 7705 SAR-M may have an integrated 16-port channelized DS1/E1 ASAP card or a module slot. The 7705 SAR-M variants are:

- fan-cooled chassis with integrated 7-port Ethernet card, integrated 16-port channelized DS1/E1 ASAP card, and module slot
- fan-cooled chassis with integrated 7-port Ethernet card and module slot
- passively cooled chassis with integrated 7-port Ethernet card and integrated 16-port channelized DS1/E1 ASAP card
- passively cooled chassis with integrated 7-port Ethernet card

The following module cards can be inserted in the module slot:

- GPON module
- DSL module
- DCM
- 1 Colour Optical Add/Drop Mux module (OADM)

The DSL module includes a port with eight XDSL lines. The DCM includes one port with four SHDSL lines and one port with two XDSL lines. Except for 802.1x, 802.1ab LLDP, line loopbacks, and LAGs, all services and limitations which apply to Ethernet ports also apply to DCM and DSL modules.

12.12 Workflow to manage 7705 SAR devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7705 SAR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 12.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM Network Element Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 13 for more information. Configure polling policies as described in Procedure 13-10.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

4 As required, manage and configure equipment; see chapter 16 for more information about equipment management and configuration. Additionally, configure the following:

- **a** ICMP extensions as described in Procedure 17-12
- **b** QoS ingress aggregate rates on the 7705 SAR-M as described in Procedure 17-13
- **c** Timing synchronization as described in Procedure 19-5
- **d** IEEE 1588 PTP clock as described in Procedures 19-6, 19-7, and 19-8
- **e** auxiliary alarm definitions as described in Procedure 19-9
- **f** channelized TDM ports as described in Procedure 20-19

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

7 Create equipment inventories of managed devices; see chapter 22 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs; see chapter 24 for more information
- **b** threshold-crossing alarms; see chapter 26 for more information
- **c** bulk configuration changes; see chapter 27 for more information
- **d** object life cycle management; see chapter 28 for more information
- **e** automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 31 for more information.
- **b** MPLS and LSPs; see chapter 32 for more information.
- **c** service tunnels to carry service traffic; see chapter 33 for more information.
- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** 5620 SAM alarm policies; see chapter 37 for more information.
- **g** OAM diagnostic tests; see chapter 38 for more information.

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 47 for more information. Additionally, configure fabric profile as described in Procedure 47-24.
- **b** filter policies; see chapter 48
- **c** multicast policies; see chapter 49 for more information
- **d** VRRP policies; see chapter 51 for more information
- **e** auto tunnels policies; see chapter 52 for more information
- **f** 802.1x policies; see chapter 54 for more information
- **g** PBB MRP policies; see chapter 55 for more information

- **h** connection profile policies; see chapter 57 for more information
- **i** service PW template policies; see chapter 58 for more information
- **j** residential subscriber policies; see chapter 59 for more information
- **k** size constraint policies; see chapter 61 for more information
- **l** NAT policies; see chapter 62 for more information
- **m** format and range policies; see chapter 63 for more information

12 Configure services and related functions; see chapters 64 and 65 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, Ipipe, and Hpipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **h** composite services to connect various types of services; see chapter 76 for more information
- **i** 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information
- **j** OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information
- **k** Ethernet Connectivity Fault Management; see chapter 80 for more information
- **l** RCA audit; see chapter 81 for more information

12.13 7710 SR support

The Alcatel-Lucent 7710 SR is a modular, multi-service edge router that aggregates subscriber traffic over a variety of interfaces. It is based on the Alcatel-Lucent 7750 SR, and is typically deployed in distributed hub sites and enterprise customer offices to extend IP services to the network edge.

The 7710 SR chassis is optimized for the delivery of data, voice and video services, and supports up to 4 or up to 12 interfaces of various types and speeds.

12.14 Workflow to manage 7710 SR devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7710 SR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 12.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 13 for more information. Configure polling policies as described in Procedure 13-10.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions; see chapter 14 for more information.

4 As required, manage and configure equipment; see chapter 16 for more information about equipment management and configuration. Additionally, configure channelized TDM ports as described in Procedure 20-20.

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 21.

6 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 23 for more information.

7 Create equipment inventories of managed devices; see chapter 22 for more information.

8 As required, perform additional device management functions such as the following:

- **a** TCP enhanced authentication between NEs; see chapter 24 for more information
- **b** threshold-crossing alarms; see chapter 26 for more information
- **c** bulk configuration changes; see chapter 27 for more information
- **d** object life cycle management; see chapter 28 for more information
- **e** automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions such as the following:

- **a** NE protocols; see chapter 31 for more information
- **b** MPLS and LSPs; see chapter 32 for more information

- **c** service tunnels to carry service traffic; see chapter 33 for more information
- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** 5620 SAM alarm policies; see chapter 37 for more information
- **g** OAM diagnostic tests; see chapter 38 for more information

10 As required, configure redundancy in the managed network using functions such as the following:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information
- **c** MC peer groups; see chapter 41 for more information
- **d** MC endpoint groups; see chapter 42 for more information
- **e** MC LAG groups; see chapter 43 for more information
- **f** MC synchronization groups; see chapter 44 for more information
- **g** MC ring groups; see chapter 45 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions; see chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as the following:

- **a** QoS policies; see chapter 47 for more information
- **b** filter policies; see chapter 48 for more information
- **c** multicast policies; see chapter 49 for more information
- **d** time of day policies; see chapter 50 for more information
- **e** VRRP policies; see chapter 51 for more information
- **f** auto tunnels policies; see chapter 52 for more information
- **g** RADIUS-based accounting policies; see chapter 53 for more information
- **h** 802.1x policies; see chapter 54 for more information
- **i** PBB MRP policies; see chapter 55 for more information
- **j** connection profile policies; see chapter 57 for more information
- **k** service PW template policies; see chapter 58 for more information
- **l** residential subscriber policies; see chapter 59 for more information
- **m** remote network monitoring policies; see chapter 60 for more information
- **n** size constraint policies; see chapter 61 for more information

- **o** NAT policies; see chapter 62 for more information
- **p** format and range policies; see chapter 63 for more information

12 Configure services and related functions; see chapters 64 and 65 for general service information. As required, configure specific services and related functions such as the following:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **h** VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 74 for more information
- **i** composite services to connect various types of services; see chapter 76 for more information
- **j** 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information
- **k** OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information
- **l** Ethernet Connectivity Fault Management; see chapter 80 for more information
- **m** RCA audit; see chapter 81 for more information

12.15 7750 MG support

The 5620 SAM supports the discovery and management of the 7- or 12-slot Alcatel-Lucent 7750 MG. The 7750 MG can be configured as an SGW or a PGW in an LTE network.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 7750 MG management. The following documents describe 5620 SAM management and configuration of the 7750 MG:

- *5620 SAM LTE ePC User Guide*—Describes 7750 MG discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes 7750 MG device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

12.16 7750 SR support

The Alcatel-Lucent 7750 SR is a multi-service edge router designed for service providers, cable MSO, and enterprise customers that deliver residential, business and mobile services through an IP/MPLS network. The 7750 SR is optimized for the high-performance delivery of data, voice and video services.

The 5620 SAM supports the following 7750 SR chassis types:

- 7750 SR-1
- 7750 SR-7
- 7750 SR-12
- 7750 SR-c4
- 7750 SR-c12

7750 SR-c4

The 7750 SR-c4, which supports up to 4 CMAs or 2 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR. The ICM-2 is a preconfigured MDA that you cannot add or delete using the 5620 SAM.

The 7750 SR-c4 supports the following CMAs and MDAs:

- 7750 SR-c4 CFM-C4-XP
- 7750 SR-c4 IOM-C4-XP
- 5-port GIGE XP SFP CMA
- 1-port GIGE XP SFP CMA
- DC PEM

7750 SR-c12

The 7750 SR-c12, which supports up to 12 CMAs or 6 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR.

12.17 Workflow to manage 7750 SR devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 7750 SR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions described in section 12.2.

1 Determine configuration requirements for the installed device; see this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2 Commission the device for 5620 SAM management; see chapter 13 for more information. Configure polling policies as described in Procedure 13-10.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions. See chapter 14 for more information.

4 As required, manage and configure equipment. See chapter 16 for more information. Additionally, configure the following:

- **a** mixed mode; see Procedure 19-4 for more information
- **b** IEEE 1588 PTP clock; see Procedures 19-6 and 19-7 for more information

5 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See chapter 21 for more information.

6 If required, perform NE maintenance functions, such as the following:

- **a** backing up and restoring device configurations
- **b** upgrading device software
- **c** monitoring deployment of configuration changes to devices

See chapter 23 for more information.

7 Create equipment inventories of managed devices. See chapter 22 for more information.

8 As required, perform additional device management functions, such as:

- **a** TCP enhanced authentication between NEs; see chapter 24 for more information
- **b** card migration; see chapter 25 for more information
- **c** threshold-crossing alarms; see chapter 26 for more information
- **d** bulk configuration changes; see chapter 27 for more information
- **e** object life cycle management; see chapter 28 for more information
- **f** automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding. See chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions, such as:

- **a** NE protocols; see chapter 31 for more information
- **b** MPLS and LSPs; see chapter 32 for more information
- **c** service tunnels to carry service traffic; see chapter 33 for more information
- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** ISA-Video; see chapter 36 for more information
- **g** 5620 SAM alarm policies; see chapter 37 for more information
- **h** OAM diagnostic tests; see chapter 38 for more information

10 As required, configure redundancy in the managed network using functions such as:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information
- **c** MC peer groups; see chapter 41 for more information
- **d** MC endpoint groups; see chapter 42 for more information
- **e** MC LAG groups; see chapter 43 for more information
- **f** MC synchronization groups; see chapter 44 for more information
- **g** MC ring groups; see chapter 45 for more information

11 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types, such as:

- **a** QoS policies; see chapter 47 for more information
- **b** filter policies; see chapter 48 for more information
- **c** multicast policies; see chapter 49 for more information
- **d** time of day policies; see chapter 50 for more information
- **e** VRRP policies; see chapter 51 for more information
- **f** auto tunnels policies; see chapter 52 for more information
- **g** RADIUS-based accounting policies; see chapter 53 for more information
- **h** 802.1x policies; see chapter 54 for more information
- **i** PBB MRP policies; see chapter 55 for more information
- **j** connection profile policies; see chapter 57 for more information

- **k** service PW template policies; see chapter 58 for more information
- **l** residential subscriber policies; see chapter 59 for more information
- **m** remote network monitoring policies; see chapter 60 for more information
- **n** size constraint policies; see chapter 61 for more information
- **o** NAT policies; see chapter 62 for more information
- **p** format and range policies; see chapter 63 for more information

12 Configure services and related functions. See chapters 64 and 65 for general service information. As required, configure specific services and related functions, such as:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **e** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **f** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information
- **g** IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information
- **h** VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 74 for more information
- **i** composite services to connect various types of services; see chapter 76 for more information
- **j** Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 77 for more information
- **k** 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions, such as running OAM diagnostics; see chapter 79 for more information
- **l** OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information
- **m** Ethernet Connectivity Fault Management; see chapter 80 for more information
- **n** RCA audit; see chapter 81 for more information

12.18 9471 MME support

The 5620 SAM allows you to view the properties of the 9471 MME equipment, instance, interface function, application function, and packet handler. The 9471 MME equipment is represented in the 5620 SAM equipment navigation tree.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 9471 MME management. The following documents describe 5620 SAM management and configuration of the 9471 MME:

- *5620 SAM LTE ePC User Guide*—Describes 9471 MME discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes 9471 MME device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

12.19 9500 MPR support

The Alcatel-Lucent 9500 MPR is a microwave digital radio that supports PDH and Ethernet to migrate from TDM to IP. The 9500 MPR provides a generic, modular IP platform for multiple network applications, such as 2G, 3G, HSDPA, and WiMAX to accommodate broadband services.

5620 SAM support for the 9500 MPR includes the following:

- 4 and 8-slot MSS shelves
- removable core-enhanced radio modem, 32 x DS1 and 32 x E1, 16 x E1 ASAP Access (ETSI) card, 2 x DS3 (ANSI) card, 4+4 x Ethernet (EAS) (ANSI) card, and cooling fan cards
- ODUs
- LAG objects

MSS-4 and MSS-8 shelves

Slots 1 and 2 are reserved for core-enhanced cards. Each shelf requires a core-enhanced card in slot 1 and can have an optional spare card installed in slot 2 to protect the main card.

The MSS-4 shelf supports cards in slots 3 and 4. The card slots can be used for unprotected radio modem or 32 x DS1 / 32 x E1 cards. A card in slot 3 can be protected by an identical card in slot 4.

The MSS-8 shelf supports six additional card slots. The slots support any combination of unprotected radio modem and 32 x DS1 / 32 xE1 cards, or a combination of protected and unprotected cards. Protected cards must be installed in slots 3, 5, or 7 and are protected by optional identical cards in slots 4, 6, and 8, respectively.

9500 MPR supported cards

The 9500 MPR supports the following card types:

Core-enhanced card

The core-enhanced card in slot 1 provides the following:

- device management and control functions
- DC power
- a plug-in flash memory card to store device configuration and license data
- an Ethernet switch that implements the cross-connections between the radio modem or 32 x DS1 / 32 x E1 cards, between the Ethernet user ports, and between the Ethernet ports and the radio modem or 32 x DS1 / 32 xE1 cards
- four electrical Ethernet ports; port 4 can be used as an additional management port, if required
- two SFP Ethernet ports; the ports are supported by the 5620 SAM when an SFP MDA is installed
- up to six MPT radio ports; ports 1 to 4 support MPT-HC, MPT-HCv2 and MPT-MC; ports 5 and 6 support MPT-HC, MPT-HCv2, and SFP

An optional identical core-enhanced card can be installed in card slot 2. The card provides protection if the card in slot 1 fails.

Core-B card

The Core-B card in slot 1 provides the following:

- device management and control functions
- DC power
- a plug-in flash memory card to store device configuration and license data
- an Ethernet switch that implements the cross-connections between the radio modem or 32 x DS1 / 32 x E1 cards, between the Ethernet user ports, and between the Ethernet ports and the radio modem or 32 x DS1 / 32 xE1 cards
- four Gigabit Ethernet electrical interfaces and one Gigabit Ethernet SFP optical interface

An optional identical core-enhanced card can be installed in card slot 2. The card provides protection if the card in slot 1 fails.

Note — The Core-B card is supported on 9500 MPR for ANSI 1.2.0 only.

Radio modem card

The radio modem card contains EPS and RPS logic, and performs the following:

- sends and receives standard Ethernet packets to and from the core-enhanced cards
- manages the radio frame generation and termination, the interface to and from the alternate radio transport card, and the cable interface functions to the ODU
- generates internal DC power for the card

32xE1(ETSI) card and 32xDS1(ANSI) card

Two 32 port cards versions are available: the 32 x E1 ETSI standard based and the 32 x DS1 ANSI standard based cards.

- provides external interfaces for up to 32 E1or DS1 ports
- manages the encapsulation and reconstruction of PDH data for standard Ethernet packets
- sends and receives standard Ethernet packets to and from core-enhanced cards
- contains the switch for EPS core protection
- generates internal dc power

2 x DS3 (ANSI) card

Two DS3 ports are available.

- supports up to six units per shelf
- 1+1 EPS protection

4+4 x Ethernet (EAS) card

The 4+4 x EAS module can be configured in any card slot on the 9500 MPR. This ANSI- based card supports 4 x Ethernet 10/100/1000-baseT (traffic) and 4+4 x Ethernet (Access/MPT) connection interfaces. Each chassis allows up to two EAS modules. ANSI 3.1 or later is supported. You can configure the 4+4 x EAS module with two types of MPT radio ports: MPT and SFP. This function is supported on ports 5 to 8.

2+2 x Ethernet (EAS) card

The 2+2 x EAS module can be configured with three types of MPT radio ports: MPT-HC, MPT-HCv2 and MPT-MC. MPP-MC can be configured only on ports 1 and 2, and cannot be involved in protection. MPT-HCs and MPT-HCv2 can be configured on any of the four ports if the corresponding port on the consecutive slot has the same card with the same MPT type. Card protection in this case is applicable. ANSI 3.1 or later is supported.

MPT-ACC ports are supported for 9500 MPR ANSI Release 3.0.0.

2 X STM card (ETSI 3.0.0 only)

The two port 2 x STM card is supported on card slots 3 and 4 only for ETSI Release 3.0.0.

16 x E1 ASAP Access (ETSI) card

The 16 x E1 ASAP Access (ETSI) card enables the management of ATM services on the 9500 MPR, through collecting IMA traffic, terminating the IMA groups and encapsulating and extracting the ATM cells into and from ATM PW packets towards the core board. ATM interfaces are established over PDH physical interfaces. ATM traffic is transported by the ATM PW service and encapsulated in Ethernet frames. The card is supported for ETSI Release 1.3.0.

2xSTM card

The 2xSTM card can be configured in all card slots on the 9500 MPR. Up to two ports can be configured. This ETSI- based card supports SFP-O and SFP-E port usage type.

1xSTM Channelized card

The 1xSTM channelized card can be configured in all card slots on the 9500 MPR. Up to one port can be configured. This ETSI- based card supports SFP-O and SFP-E port usage type. Up to 63E1 channels are supported. Services are deployed at the E1 channel level as TDM over Ethernet.

ODU

The ODU is a microprocessor-controlled transceiver that interfaces the MSS with the microwave antenna. Each radio modem card connects to one ODU. A 1 + 0 radio modem protection scheme requires one radio modem card and one ODU for each radio direction. Two radio modem cards and two associated ODUs must be provisioned in each radio direction for the 1+1 protection scheme.

XPIC

XPIC is an ODU which draws power and data from a 2+2 x Ethernet (EAS) card when the port is configured as MPT-HC. See Procedure 20-29 to configure power source type over Ethernet on a 2+2 x Ethernet (EAS) card. See Procedure 20-26 to configure MPT radio ports for SFP, MPT-HC. See the 9500 MPR user documentation for more information about how to install and use the NEtO software to configure XPIC.

9500 MPR LAG objects

The 5620 SAM can discover 9500 MPR LAG objects, but the LAG properties are not configurable using the GUI. All LAGs and their corresponding port terminations are created using CLI. The 5620 SAM does not allow creation, modification, or deletion of LAG properties or port terminations. See Procedure 18-17 to configure the Service creation and discovery associated with 9500 MPR Radio LAGs or Ethernet LAGs.

Port terminations are not discovered if the LAG type is Ethernet. If an Ethernet port is associated with a LAG, the port properties are read-only; modification using the 5620 SAM is not possible. An Ethernet LAG is in network mode and cannot be used in the 9500 MPR Release 3.1.0. Service creation is not possible using an Ethernet LAG as a network port.

You can associate only an MPT port as a LAG member. The following MPT ports can be configured using CLI:

- MPT MC
- MPT HC
- MPT HL

LAG objects support the following port types in 9500 MPR Release 3.2.0:

- MPT-HC
- MPT-MC
- MPT-HL
- MD300
- Ethernet

Using the 9500 MPR external element manager

You can start the 9500 MPR external element manager, NEtO, from the 5620 SAM GUI. See the 9500 MPR user documentation for information about installing and using the NEtO NE manager. See chapter 17 for information about starting the external element manager from the 5620 SAM GUI.

9500 MPR backups and restores

After 5620 SAM discovery, 9500 MPR NEs are automatically assigned to the default MPR Backup Policy and the MPR Read/Write Policy.

The MPR Read/Write Policy is a mediation policy that is automatically created. It contains the default FTP authentication details which have to be configured using the FTP login credentials required for backup and restore access. BOF save and CLI are not supported on 9500 MPR NEs. See chapter 23 for information about creating a 9500 MPR backup policy.

12.20 Workflow to manage 9500 MPR devices

The following workflow describes the sequence of high-level tasks required to configure and manage end-user 9500 MPR NEs and services. This workflow assumes that the physical devices have been installed. The management functions are supplemental to the general management functions. See section 12.2 for more information.

1. Determine the configuration requirements for the installed device. See this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for device specific information.

2. Enable 5620 SAM management of a 9500 MPR; see Procedure 13-15 for more information.

3. Configure the required polling policies for a 9500 MPR; see Procedure 13-13 for more information.

4. Start the 9500 MPR external element manager (NEtO) from the 5620 SAM GUI; see Procedure 17-14 for more information.

5 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions. See chapter 14 for more information.

6 As required, manage and configure equipment. See chapter 16 for more information about equipment management and configuration. Additionally, configure the following, as required:

  a manage the software in the 9500 MPR committed and standby banks; see Procedure 19-12 for more information

  b card and port protection; see Procedures 19-19, 19-20, 20-31, and 20-32 for more information

  c ports; see Procedures 20-21, 20-22, 20-23, 20-24, 20-25, 20-26, 20-27, 20-28, 20-30, and 20-33 for more information

  d power source type on EAS card slots; see Procedure 20-29 for more information

  e radio LAGs or Ethernet LAGs; see Procedures 18-17 and 18-18 for more information

7 Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication. See chapter 21 for more information.

8 If required, perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices. See Workflow for a 9500 MPR software upgrade in chapter 23 for more information.

9 Create equipment inventories of managed devices. See chapter 22 for more information.

10 As required, perform additional device management functions, such as:

  a TCP enhanced authentication between NEs; see chapter 24 for more information

  b threshold-crossing alarms; see chapter 26 for more information

  c bulk configuration changes; see chapter 27 for more information

  d object life cycle management; see chapter 28 for more information

  e automatic provisioning; see chapter 29 for more information

11 Configure NE routing and forwarding; see chapter 30 for general routing and forwarding information. As required, configure specific routing and forwarding functions, such as:

  a NE protocols; see chapter 31 for more information

  b MPLS and LSPs; see chapter 32 for more information

  c service tunnels to carry service traffic; see chapter 33 for more information. Additionally, configure Ethernet radio ring elements; see Procedure 33-9 for more information

- **d** Lawful Intercept; see chapter 34 for more information
- **e** IPsec; see chapter 35 for more information
- **f** error recovery mechanisms; see Procedure 37-21 for more information. See chapter 37 for more information about configuring 5620 SAM alarm policies.
- **g** OAM diagnostic tests; see chapter 38 for more information

12 As required, configure redundancy in the managed network using functions such as:

- **a** VRRP; see chapter 39 for more information
- **b** APS; see chapter 40 for more information

13 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types, such as:

- **a** ATM QoS policies; see Procedure 47-32 for more information. See chapter 47 for more information about QoS policies.
- **b** radio interface queue map policies; see Procedure 47-33 for more information.
- **c** NE QoS policies; see Procedure 47-34 for more information.
- **d** filter policies; see chapter 48 for more information
- **e** multicast policies; see chapter 49 for more information
- **f** VRRP policies; see chapter 51 for more information
- **g** auto tunnels policies; see chapter 52 for more information
- **h** 802.1x policies; see chapter 54 for more information
- **i** PBB MRP policies; see chapter 55 for more information
- **j** connection profile policies; see chapter 57 for more information
- **k** service PW template policies; see chapter 58 for more information
- **l** residential subscriber policies; see chapter 59 for more information
- **m** size constraint policies; see chapter 61 for more information
- **n** NAT policies; see chapter 62 for more information
- **o** format and range policies; see chapter 63 for more information

14 Configure services and related functions. See chapters 64 and 65 for general service information. As required, configure specific services and related functions, such as:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information

c residential subscribers of customer services; see chapter 68 for more information

d 9500 MPR (dot1q) VLAN services; see Procedure 69-8 for more information.

e VLAN groups and VLAN paths; see Procedures 69-10 and 69-12 for more information

f VLL Apipe, Cpipe, and Epipe services to provide point-to-point connectivity between customer access ports; see Procedures 70-3, 70-5, and 70-10 for more information.

g VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information.

h composite services to connect various types of services; see chapter 76 for more information

i 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information

j OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information

k Ethernet Connectivity Fault Management; see chapter 80 for more information

l RCA audit; see chapter 81 for more information

12.21 eNodeB support

The eNodeB is an enhanced BTS system for UE access to the LTE RAN network and LTE services in the 700 MHz spectrum. The eNodeB is available as a compact or distributed system that consists of a BBU and a compact TRDU or distributed RRH component.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe eNodeB management. The following documents describe 5620 SAM management and configuration of the eNodeB:

- *5620 SAM LTE RAN User Guide*—Describes eNodeB discovery, configuration, and management using the 5620 SAM
- *5620 SAM LTE Parameter Reference*—Describes eNodeB device MIM parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI

Note — The *5620 SAM Alarm Reference* lists and describes all 5620 SAM alarms, including LTE and optical alarms.

12.22 OmniSwitch support

The Alcatel-Lucent OmniSwitch family of devices is a group of enterprise LAN switches. The 5620 SAM supports the OmniSwitch chassis types listed in Table 12-1.

Table 12-1 5620 SAM OmniSwitch support

Family	Characteristics	AOS Version Supported	Chassis and cards support
OS 6250	Layer 2+ Fast Ethernet Stackable LAN family of switches for both the enterprise (SME) and Ethernet (Metro) access segments.	Release 6.6.1 or later	Non-PoE chassis • OS 6250-24 • OS 6250-8M • OS 6250-24M • OS 6250-24MD PoE chassis • OS 6250-P24
OS 6400	Stackable layer 2+ gigabit Ethernet LAN switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	Release 6.3.3 or later	Non-PoE chassis • OS6400-24 • OS6400-48 PoE chassis • OS6400-P24 • OS6400-P48 Fiber chassis • OS6400-U24 • OS6400-U24D
OS 6850	Stackable layer 2/3 gigabit Ethernet fixed configuration switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	Release 6.3.1 or later	Non-PoE chassis • OS6850-24 • OS6850-24X • OS6850-48 • OS6850-48X • OS6850-U24X • OS6850-24L • OS6850-48L PoE chassis • OS6850-P24 • OS6850-P24X • OS6850-P48 • OS6850-P48X • OS6850-P24L • OS6850-P48L

(1 of 3)

Family	Characteristics	AOS Version Supported	Chassis and cards support
OS 6850E	The OS 6850E is the next evolution of the OS 6850. In addition to supporting the features of the OS 6850, the areas of enhancements for OS 6850E include form factor, new transceiver support, and new stacking mode.	Release 6.4.4 or later	Non-PoE chassis • OS 6850E-24 • OS 6850E-24X • OS 6850E-48 • OS 6850E-48X • OS 6850E-U24X PoE chassis • OS 6850-P24 • OS 6850E-P24X • OS 6850E-P48 • OS 6850E-P48X
OS 6855	Stackable layer 2/3 gigabit Ethernet switch specifically built for IP network deployments where environmental operating conditions are unusually demanding. The OS 6855 is available with up to 24 gigabit ports and four combo ports.	Release 6.3.2 or later Stackability only among OS6855-U24X chassis, Release 6.4.2	Fiber chassis • OS6855-U10 • OS6855-U24 • OS6855-U24X (stackable) Copper with Po E chassis • OS6855-14 • OS6855-24
OS 6900	The OS 6900 is a family of standalone aggregation switches that consists of two models: the OS 6900-X20 (640 Gb/s) and the OS 6900-X40 (1.28 Tb/s). The OS 6900-X40 has 40 fixed SFP+ ports, and two expansion slots. The OS 6900-X20 has 20 fixed SFP+ ports, and one expansion slot. Both models provide 1+1 redundant hot-swappable power supplies and a field-replaceable fan tray. Each expansion slot is capable of supporting 120 Gb/s of bandwidth.	Release 7.2.1 or later	XNI cards (supported on both model types) • OS-XNI-U12: Supports 12 SFP+ ports • OS-XNI-U4: Supports 4 SFP+ ports
OS 9600	A five-slot chassis supporting one CMM and four network interface modules. It offers a wide range of GigE and 10GigE interfaces and power-over-Ethernet to support IP telephones, WLAN access points and video cameras. The OS 9600 supports a maximum of two load sharing power supplies.	Release 6.3.1 R2 or later	CMM cards • OS9600-CMM • OS9700-CMM • OS9800-CMM Network interface cards • 2-port 10GigE XFP • 6-port 10GigE XFP • 20-port Fast Ethernet (10/100 – SW upgradable to 10/100/1000) RJ45 and 2-port GigE (100/1000) SFP • 24-port GigE SFP • 24-port GigE (10/100/1000) RJ45 • 24-port GigE (10/100/1000) RJ45 w/PoE • OS9-GNI-P24: 24-port (10/100/1000) TX (RJ-45) PoE support • 48-port GigE (10/100/1000) MRJ21
OS 9700	A high-density ten-slot chassis with two slots for control and eight slots for network interfaces supporting an aggregation of up to 192 GigE ports or 48 10GigE ports. Designed for smart continuous switching operation, the two center slots are dedicated to CMMs allowing redundant configurations. The OS 9700 supports a maximum of three power supplies.	Release 6.3.1 R2 or later	
OS 9800	A high performance 18-slot switch supporting 16 slots for Gigabit Ethernet and/or 10-Gigabit Ethernet network interface modules. An additional two slots are reserved for primary and redundant CMMs. The OS 9800 supports a maximum of four power supplies.	Release 6.3.1 R2 or later	

(2 of 3)

Family	Characteristics	AOS Version Supported	Chassis and cards support
OS 9700E	The OS 9700E is a high performance switch offering eight slots for Gigabit Ethernet and/or 10-gigabit Ethernet Network Interface (NI) modules. Additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).	Release 6.4.4 R1 or later	Network interface cards • OS9-GNI-C24E: 24-port 10/100/1000 with RJ-45 support • OS9-GNI-U24E: 24-port 1000base-X with SFP/MiniGBIC support • OS9-GNI-P24E: 24-port (10/100/1000) T/TX (RJ-45) PoE+ support • OS9-XNI-U2E: 2-port unpopulated 10-Gigabit Ethernet with XFP support
OS 9800E	The OS 9800E is a high performance switch offering 16 slots for Gigabit Ethernet and/or 10-Gigabit Ethernet Network Interface (NI) modules. An additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).		
OS 10K(1)	The OS 10K is a high-capacity, high-performance modular Ethernet LAN switch that provides 5.12 Tb/s of switching performance. The OS 10K has a 12 slot chassis configuration: 4 slots for CMM/fabric cards; and 8 slots for XNI or GNI cards that provide Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet capabilities.	Release 7.1.1 or later	CMM and CFM cards • OS10K-CMM • OS10K-CFM XNI cards • OS10K-XNI-U32S: 32 unpopulated 10G SFP+ transceiver connectors GNI cards • OS10K-GNI-U48E: 48 SFP transceiver connectors • OS10K-GNI-C48E: 48 auto-sensing ports, each port is configurable as 10BaseT, 100BaseTX, or 1000BaseT

(3 of 3)

Note

(1) The behavior of the power supplies is controlled by power management. You will see a power failure alarm even though power supplies are connected to the OS 10K chassis and is not being used by the 10K node. The 10K power management puts power supply into an inactive (down) state, if it is not required.

Caution 1 — OmniSwitch devices do not support automatic synchronization with the 5620 SAM database when you use the CLI to make configuration changes. To ensure that you are viewing accurate OmniSwitch information in the 5620 SAM, you must resynchronize the NE by clicking on the appropriate Resync button.

Caution 2 — OmniSwitch NEs do not send trap notifications for all MIB changes on the NE. To ensure that you are viewing the current configuration information in the 5620 SAM, you must resynchronize of the NE by clicking on the appropriate Resync button.

OmniSwitch LAG objects

OmniSwitch devices support static and dynamic LAGs. When you create a static LAG, you can manually add ports as LAG members. The ports that you select as members of a dynamic LAG are first placed into an Unassigned Dynamic LAG Members group. The OmniSwitch uses LACP to dynamically assign ports from an Unassigned Dynamic LAG Members group to the appropriate LAG. When a port is assigned to a dynamic LAG, it is removed from the Unassigned Dynamic LAG Members group.

You can create VLANs, use 802.1Q framing, configure QoS conditions, and enable other networking functions on a LAG, which is treated like a physical link.

OmniSwitch LAG support includes the following:

- up to 32 LAGs on an OS 6250, OS 6400, OS 6850, OS 6850E, or OS 6855 or stack of OmniSwitch devices
- up to 128 LAGs on an:
    - OS 9600, OS 9700, OS 9800, Release 6.3.4 or later
    - OS 9700E or OS 9800E, Release 6.4.2 or later
    - OS 6900, Release 7.2.1 or later
    - OS 10K, Release 7.1.1 or later
- two, four, or eight Ethernet links in a LAG
- access or network LAGs

Using WebView to manage an OmniSwitch

You can configure and manage an OmniSwitch using the WebView application, an Alcatel-Lucent web-based element management tool that runs on an OmniSwitch. WebView supports the following web browsers:

- Internet Explorer 6.0 or later for Windows
- Netscape 7.1 for Windows
- Netscape 7.0 for Solaris

Note — The web browser must have cookies and Java enabled.

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using WebView. See chapter 17 for information about opening WebView using the 5620 SAM GUI.

12.23 Workflow to manage OmniSwitch devices

The following workflow describes the sequence of high-level tasks that are required to configure and manage end-user OmniSwitch NEs and services. The workflow assumes that the physical devices are installed. The management functions are supplemental to the general management functions described in section 12.2.

1 Determine the configuration requirements for installed devices. See this chapter, the *5620 SAM NE Compatibility Guide*, and the *5620 SAM Parameter Guide* for specific device information.

2 Commission the device for 5620 SAM management. See Procedure 13-4 and chapter 13 for more information.

3 Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions. See chapter 14 for more information.

4 As required, manage and configure equipment. See chapter 16 for more information about equipment management and configuration. Additionally, configure:

- **a** LAGs; see Procedures 18-15 and 18-16 for more information.
- **b** PoE ports; see Procedure 19-21 for more information.
- **c** Ethernet ports; see Procedure 20-34 for more information.
- **d** stacks; see Procedure 19-22 for more information.
- **e** CPU temperature threshold; see Procedure 19-23 for more information.
- **f** LLDP; see Procedures 17-9 and 20-34 for more information.
- **g** running configuration; see Procedure 19-13 for more information.
- **h** health monitoring; see Procedure 19-14 for more information.
- **i** Ethernet diagnostics; see Procedures 17-16, 17-17, and 17-18 for more information.

5 Create RADIUS or TACACS+ security policies. See Procedure 21-11 and chapter 21 for more information.

6 If required, perform NE maintenance functions, such as:

- **a** backing up and restoring device configurations; see chapter 23 for more information
- **b** upgrading device software; see chapter 23 for more information
- **c** monitoring deployment of configuration changes to devices; see chapter 23 for more information
- **d** immediate software upgrade; see Procedure 23-16 for more information

7 Create equipment inventories of managed devices. See chapter 22 for more information.

8 As required, perform additional device management functions, such as:

   a TCP enhanced authentication between NEs; see chapter 24 for more information

   b threshold-crossing alarms; see chapter 26 for more information

   c bulk configuration changes; see chapter 27 for more information

   d object life cycle management; see chapter 28 for more information

   e automatic provisioning; see chapter 29 for more information

9 Configure NE routing and forwarding. See chapter 30 for general routing and forwarding information. Additionally, configure the following, as required:

   a OmniSwitch routing instances; see Procedure 30-3 for more information

   b UDP relay and DHCP Snooping on OmniSwitch routing instances; see Procedure 30-6 for more information

   c OmniSwitch L3 interfaces; see Procedures 30-8 and 30-10 for more information.

   d OmniSwitch static routes; see Procedure 30-21 for more information

10 As required, configure additional specific routing and forwarding functions, such as:

   a NE protocols; see chapter 31 for more information. Additionally, configure:

      - IGMP; see Procedure 31-38 for more information
      - bridging; see Procedures 31-54 and 31-55 for more information

   b MPLS and LSPs; see chapter 32 for more information

   c service tunnels to carry service traffic; see chapter 33 for more information. Additionally, configure Ethernet ring elements; see Procedure 33-8 for more information.

   d Lawful Intercept; see chapter 34 for more information

   e IPsec; see chapter 35 for more information

   f 5620 SAM alarm policies; see chapter 37 for more information

   g OAM diagnostic tests; see chapter 38 for more information. Additionally, configure ping and traceroutes; see Procedures 38-38, 38-40, and 38-41 for more information

11 As required, configure redundancy in the managed network using functions such as:

   a VRRP; see chapter 39 for more information

   b APS; see chapter 40 for more information

12 Create 5620 SAM policies that define the conditions for 5620 SAM management functions. See chapter 46 for general information about 5620 SAM policy management. As required, configure specific policy types such as:

- **a** QoS policies; see Procedures 47-36, 47-37, and 47-38, and chapter 47, for more information.
- **b** filter policies; see chapter 48 for more information
- **c** multicast policies; see chapter 49 for more information
- **d** VRRP policies; see chapter 51 for more information
- **e** auto tunnels policies; see chapter 52 for more information
- **f** 802.1x policies; see chapter 54 for more information
- **g** PBB MRP policies; see chapter 55 for more information
- **h** AOS Ethernet service policies; see chapter 56 for more information
- **i** connection profile policies; see chapter 57 for more information
- **j** service PW template policies; see chapter 58 for more information
- **k** residential subscriber policies; see chapter 59 for more information
- **l** size constraint policies; see chapter 61 for more information
- **m** NAT policies; see chapter 62 for more information
- **n** format and range policies; see chapter 63 for more information

13 Configure services and related functions. See chapters 64 and 65 for general service information. As required, configure specific services and related functions such as:

- **a** virtual ports; see chapter 66 for more information
- **b** customers; see chapter 67 for more information
- **c** residential subscribers of customer services; see chapter 68 for more information
- **d** VLAN services; see Procedures 69-4, 69-6, 69-14, and 69-15, and chapter 69, for more information
- **e** VLAN groups and paths; see chapter 70 for more information
- **f** VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 70 for more information
- **g** VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 71 for more information
- **h** mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 72 for more information

i IES to provide an IP interface between customer traffic and the Internet; see chapter 73 for more information

j composite services to connect various types of services; see chapter 76 for more information

k 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 79 for more information

l OAM diagnostic tests into suites of manual and automatically-generated tests using the Service Test Manager; see chapter 78 for more information

m Ethernet Connectivity Fault Management; see Procedure 80-4 and chapter 80 for more information

n RCA audit; see chapter 81 for more information

12.24 Generic NE support

The 5620 SAM provides limited management support of generic NEs, which are non-Alcatel-Lucent devices, using generic NE profiles, alarm catalogues, and CLI scripts. A generic NE profile includes the following elements:

- the device MIB system object ID
- regular-expression strings that specify the format of prompts and commands
- the SNMP trap management configuration
- interfaces that can be specified as the endpoints of 5620 SAM physical links
- an optional alarm catalogue, which defines the alarms that the 5620 SAM raises in response to SNMP traps from the generic NE

Note 1 — By default, only the 5620 SAM admin user, or an operator with an assigned admin scope of command role, can manage generic NE profiles and alarm catalogues. A non-admin user requires the genericne scope of command role to manage generic NE profiles.

Note 2 — To create, modify, or delete a generic NE alarm catalogue or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

See chapter 13 for information about configuring a generic NE profile.

Generic NE device discovery and polling in the 5620 SAM are configured using the same methods that are used for an Alcatel-Lucent NE, but the 5620 SAM uses preconfigured scripts to manage and unmanage a generic NE. See chapter 11 for information about device discovery. See chapter 27 for information about creating CLI scripts using the 5620 SAM script manager.

The 5620 SAM displays generic NEs, but not generic NE interfaces, on the topology map and in the navigation tree.

Statistics support

The 5620 SAM supports the collection of a limited set of statistics counters from standard system, interface, and routing MIBs on generic NEs. These statistics are processed and presented in the same manner as statistics from other devices. You can view generic NE statistics on the Statistics tab of a generic NE interface properties form, retrieve them using the OSSI, and display them graphically using the 5620 SAM Statistics Plotter.

Note 1 — To collect or view generic NE statistics from routing MIBs, you require a valid 5650 CPAM license that has a third-party router quantity greater than zero.

Note 2 — If persistent SNMP indexes are not enabled on a generic NE, one or more generic NE interface indexes may change after a generic NE reboots. This can cause a mismatch between the statistics records collected before the reboot and the current interface indexes. The 5620 SAM takes no action to identify or correct such a mismatch.

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

Alarm support

By default, the 5620 SAM supports a limited number of standard system and interface SNMP traps for generic NEs. The 5620 SAM monitors SNMP reachability and interface status, and raises a standard alarm for each the following events:

- coldStart—The generic NE restarts.
- linkDown—An interface goes out of service.
- linkUp—An interface returns to service.

Note — When the 5620 SAM drops or fails to receive an SNMP trap from a generic NE, the trap is lost. The 5620 SAM is unable to request that a generic NE resend an SNMP trap.

You can configure the 5620 SAM to raise user-defined alarms in response to specific generic NE traps using alarm catalogues. An alarm catalogue is a set of trap-to-alarm mappings that can be associated with a generic NE profile. A generic NE profile can have at most one alarm catalogue, but each catalogue can contain up to 150 alarm mappings. When a mapping is administratively disabled, the 5620 SAM raises no alarm in response to an associated trap from a generic NE.

An alarm mapping can be static, which means that it maps to a specific alarm, or the mapping can use one or more transform functions that extend the mapping customization. A transform function defines conditions that enable the dynamic mapping of a trap to an alarm that is created using varbind values in an SNMP trap PDU. For example, you can use a transform function to assign a specific alarm name, severity, or probable cause to an alarm based on varbind values.

You can use a 5620 SAM GUI or OSS client to configure generic NE alarm catalogues and alarm mappings. The GUI supports the following methods:

- configuration forms—for object creation, modification, viewing, and deletion

  See chapter 13 for information about managing generic NE alarm catalogues using configuration forms.
- XML API script—for object creation and modification only

  A script template for alarm catalogue configuration is available at the following location:

  install_dir/nms/sample/xmlapi/AlarmCatalogue-Template.txt

  where *install_dir* is the 5620 SAM main server installation directory, typically /opt/5620sam/server

See the *5620 SAM Scripts and Templates Developer Guide* for information about using the Script Manager.

An OSS client can also retrieve a catalogue or a subset of the alarm mappings in a catalogue using the standard methods.

When the 5620 SAM receives a generic NE trap that is not one of the supported standard traps or a mapped trap in an alarm catalogue, the 5620 SAM drops the trap. When the 5620 SAM receives a high trap volume and must discard traps that it cannot process, it does not distinguish between standard and user-defined traps. To conserve system resources, Alcatel-Lucent recommends that you configure a generic NE to send only the required traps to the 5620 SAM.

Traps that map to user-defined alarms require extra processing by the 5620 SAM and are managed in a separate, resource-limited queue. When this queue fills, the 5620 SAM discards some of the traps and raises an alarm. You can monitor the queue length using the 5620 SAM Resource Manager.

Generic NE trap sequencing and throttling support are configurable in a generic NE profile. After the 5620 SAM finishes throttling traps from a generic NE or encounters a trap sequence error, it resynchronizes the discovered device MIBs.

13 — Device commissioning and management

13.1 Device commissioning overview

An Alcatel-Lucent device, Telco device, or generic NE requires commissioning preconfiguration before the 5620 SAM can manage it. When this preconfiguration is complete, the 5620 SAM can discover the device, as described in chapter 14.

Some devices, such as the 7210 SAS-E and 9500 MPR, require configuration in addition to device commissioning before the 5620 SAM can discover or manage them. See section 13.2 for information about device-specific management requirements.

Commissioning generic NEs for 5620 SAM management

The 5620 SAM uses configurable profiles and CLI configuration scripts to discover and manage generic NEs. You can use the same generic NE profile for multiple devices of the same type. Before the 5620 SAM can discover a generic NE using a discovery rule, the following conditions must be true:

- The device preconfiguration is complete.
- A 5620 SAM generic NE profile for the device exists.
- A 5620 SAM mediation policy is configured with a community string that matches the community string specified during the device preconfiguration.
- A discovery rule is configured to represent the device.

See chapter 14 for information about mediation policies and device discovery. See section 13.2 for information about configuring user-defined alarms for generic NE management.

Note 1 — By default, only the 5620 SAM admin user or an operator with an assigned admin scope of command role can manage generic NE profiles and alarm catalogs. A non-admin user requires an assigned generic NE scope of command role to manage generic NEs.

Note 2 — When multiple generic NE profiles contain possible matches for a system object ID, the profile that contains the system object ID with the longest or most specific match is chosen.

Note 3 — To create, modify, or delete a generic NE alarm catalog or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

13.2 Device management overview

The 5620 SAM supports in-band and out-of-band management of devices.

When you configure in-band management only, management traffic between the 5620 SAM and a device is transmitted through any port that is configured for network access, but not the management port. Using in-band management, the 5620 SAM sends management traffic to the system IP address of the device, or to an optional L3 management interface.

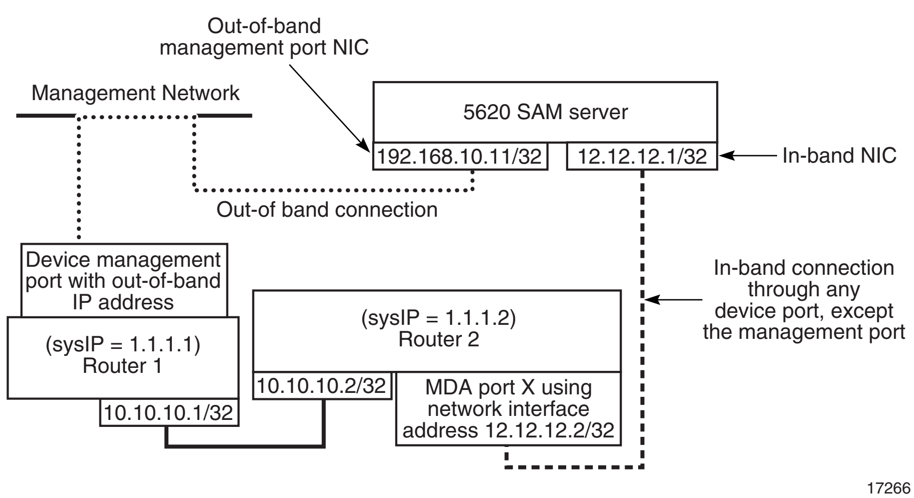
When you configure out-of-band management only, management traffic between the 5620 SAM and a device is transmitted through the management port of the device. Using out-of-band management, the 5620 SAM sends management traffic to the management IP address of the device.

When you configure a device for in-band and out-of-band management, one method provides redundancy for the other. If the IP addresses are the same, redundancy is not supported. Redundancy is not supported on the OmniSwitch.

Figure 13-1 shows an example of in-band and out-of-band management.

Note — To enable in-band management of a device, you must manually configure a second trap destination and trap log on the device.

Figure 13-1 Example of in-band and out-of-band management



The type of management is determined during device discovery. When the device is discovered using its management IP address, management is out of band. When the device is discovered using its system IP address or an L3 interface IP address, management is in band. In each case, a valid route to the device must exist. See chapter 14 for more information about the discovery process.

In Figure 13-1, there is an out-of-band management route that allows a ping from the 5620 SAM to the management IP address of router 1 (192.168.10.1/32). The in-band connection sends management packets to the system IP address on router 2 (12.12.12.2/32) on MDA port X.

Caution — Do not use the 5620 SAM to alter the configuration of the in-band port. If the port is shut down, network visibility is lost.

Some device types require configuration in addition to the SNMP configuration before they can be managed by the 5620 SAM. See the appropriate part of this section for device-specific management information.

Firewalls and management bandwidth

The ports between 5620 SAM components, and between the 5620 SAM system and the managed devices, must be open through firewalls to allow proper operation of the software. See the *5620 SAM Planning Guide* for more information about requirements for the following:

- firewalls and open ports
- communication bandwidth between 5620 SAM components
- communication bandwidth between the 5620 SAM and managed network

IPv6 management

The 5620 SAM supports device management using IPv6 for devices with IPv6 capabilities. The management protocol is established when the device is discovered. When a device is configured with an IPv6 address on its management port and/or system interface and the discovery rule is configured to discover IPv6 addresses, the 5620 SAM discovers and manages the device using IPv6. To change a device management protocol between IPv4 and IPv6, you must unmanage the device, create a new discovery rule specifying the new management protocol, and then rediscover the device.

Note — To manage 7750 SR, 7710 SR, or 7450 ESS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

The 5620 SAM supports the configuration of IPv4 and IPv6 in-band and out-of-band management addresses on the same device.

Secure file transfers

The 5620 SAM supports secure and non-secure file transfers for backups, restores, software upgrades, and statistics collection. The device mediation policy determines whether FTP or SCP is used to perform file transfers to and from the managed devices. See chapter 14 for more information about configuring SSH2.

The following devices support the use of SSH2 for secure file transfers:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6850E
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E

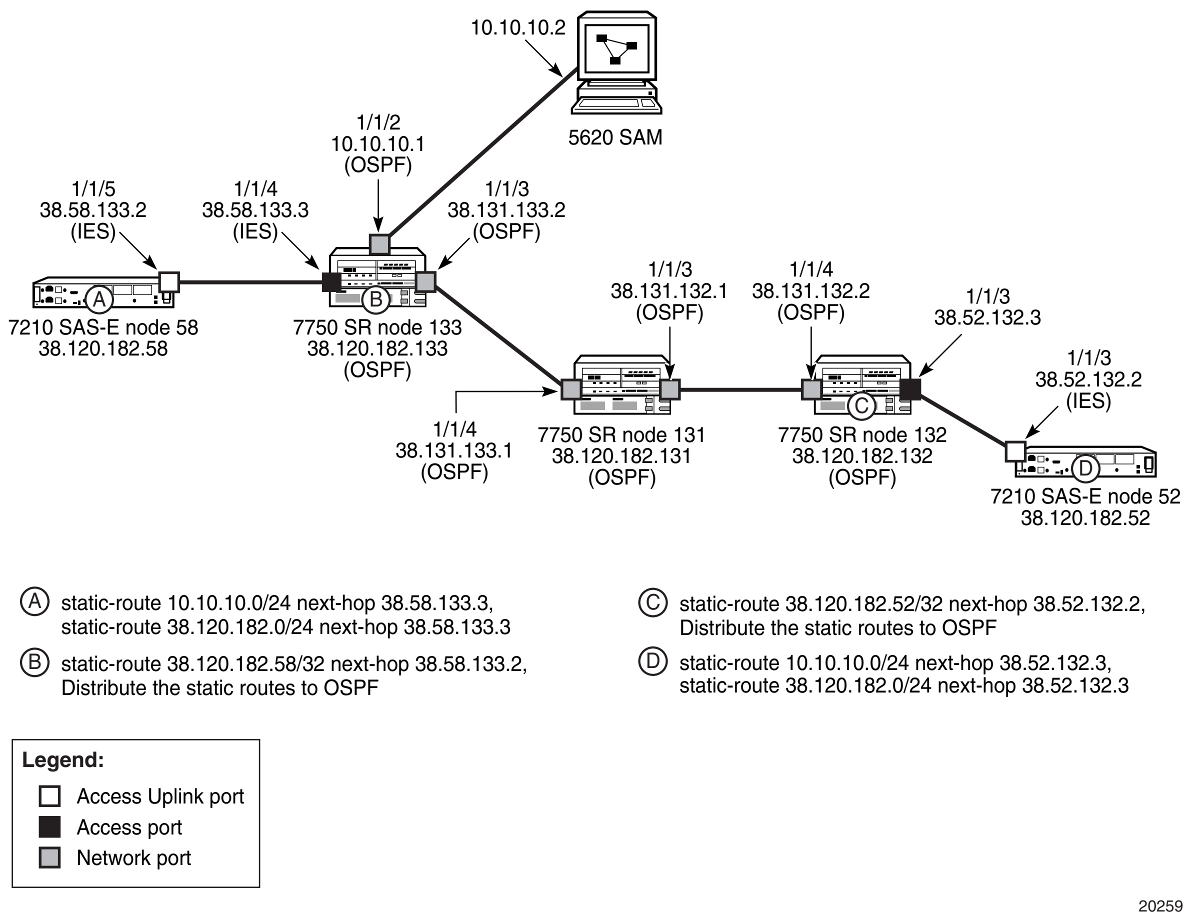
7210 SAS in-band and out-of-band management

The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP support in-band and out-of-band management. The 7210 SAS-D 6F 4T, 7210 SAS-D 6F 4T ETR, and 7210 SAS-E support static routes, but do not support an IGP or SDPs. The example network shown in Figure 13-2 and the associated configuration steps describe the configuration required to enable 7210 SAS-E in-band management using static routes that are distributed to an IGP, which, in the example, is OSPF.

Note 1 — The 7210 SAS-E Release 2.0 R2 or later supports out-of-band management.

Note 2 — The 7210 SAS-M Release 2.0 R2 or later supports out-of-band management.

Figure 13-2 Example 7210 SAS-E in-band management network



The following configuration steps are required to set up the example network:

1 Using the CLI, configure the SNMP security parameters on the devices that you need to discover. See Procedure 13-1 for more information.

2 Perform the following steps on node 133:
- Configure an interface on port 1/1/2 that connects to the 5620 SAM server interface.
- Configure an interface on port 1/1/3, which is connected to node 131.
- Create an L3 interface on port 1/1/4 by creating an IES.
- Create a static route to node 58.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interfaces to node 131 and the 5620 SAM server.
- Create a routing policy to distribute the static route to OSPF.

3 Perform the following steps on node 131:
- Configure an L3 interface on port 1/1/4, which is connected to node 133.
- Configure an L3 interface on port 1/1/3, which is connected to node 132.
- Enable OSPF (area 0.0.0.0) on the system and the interfaces connected to nodes 133 and 132.

4 Perform the following steps on node 132:
- Create an L3 interface on port 1/1/4, which is connected to node 131.
- Create an L3 interface on port 1/1/3, which is connected to node 52.
- Create a static route to node 52.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interface to node 131.
- Create a routing policy to distribute the static route to OSPF.

5 Perform the following steps on node 52:
- Create an IES L3 interface on port 1/1/3, which is an uplink port.
- Create static routes that direct traffic to the IES L3 interface.

6 Perform the following steps on node 58:
- Create a IES L3 interface on port 1/1/5, which is configured as an uplink port.
- Create static routes to direct traffic to the IES L3 interface.

7 Ensure that each 7210 SAS-E can ping the network interface IP address which is configured on the 5620 SAM main server.

8 Ensure that the 5620 SAM main server can ping the system IP address of each 7210 SAS-E.

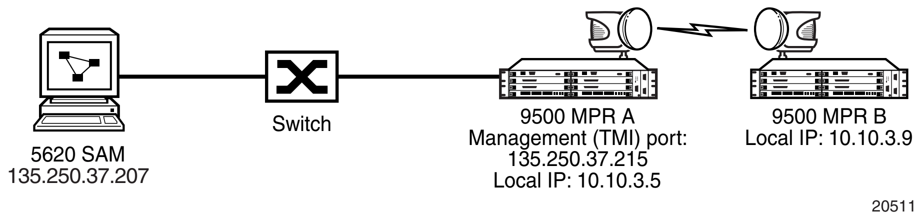
9 Configure an in-band polling policy using the 5620 SAM. See Procedure 13-12 for more information.

9500 MPR in-band management

The 9500 MPR nodes support in-band and out-of-band management.

To enable 9500 MPR in-band management, the 5620 SAM requires connectivity to the 9500 MPR NE, as shown in Figure 13-3 and described in the associated example configuration steps.

Figure 13-3 Example of 9500 MPR In-band management



Perform the following initial configuration on the 9500 MPR:

1 Connect the first 9500 MPR Node 1 to the switch using the TMN port or port 4 of the 9500 MPR A.

When the 5620 SAM is connected to the 9500 MPR network via non 9500 MPR devices like the 7705 SAR or 7750 SR, it is expected that the TMN in-band feature will be enabled on Node 1 of the 9500 MPR that is connected to non 9500 MPR devices. For example, SAM-----7705SAR_1/1/1-----port1/4_MPR1 -------(radio)------MPR2.......

In the above example, the 9500 MPR Node 1 and port 1/4 has been enabled with VLAN ID and IP addresses and the 7705 SAR is configured with the same VLAN and IP address from the same subnet.

2 Ensure that the radio links between the 9500 MPRs is working by pinging the local IP addresses. A connection between two 9500 MPR nodes could be over an Ethernet or optical link. If the core Ethernet or core optical port is used between two 9500 MPRs, the ports should be enabled with TMN in-band on the 9500 MPR.

Note — The management port IP, TMN in-band IP and local IP can be in a different subnet.

Perform the following network configuration:

1 Verify that you can ping the local IP address of all the nodes from the 5620 SAM server.

2 Verify that you can ping the 5620 SAM server IP from each of the 9500 MPR nodes.

Note — You can manage the 9500 MPR through the local IP address even though the management interface via the 5620 SAM server is not reachable.

3 The 5620 SAM should be able to discover and manage the local IP addresses of the 9500 MPRs after connectivity has been established between the 5620 SAM and the 9500 MPR nodes. See “9500 MPR support” for more information about 9500 MPR node discovery and management.

9500 MPR radio link discovery and management

The 5620 SAM supports N x (1+x) radio [x = 0, 1] link discovery. To enable 9500 MPR radio link discovery and management, the 5620 SAM requires connectivity between the 9500 MPR NE radio ports, as shown in Figure 13-4 and described in Table 13-1.

Figure 13-4 Connectivity example for 9500 MPR radio link discovery and management

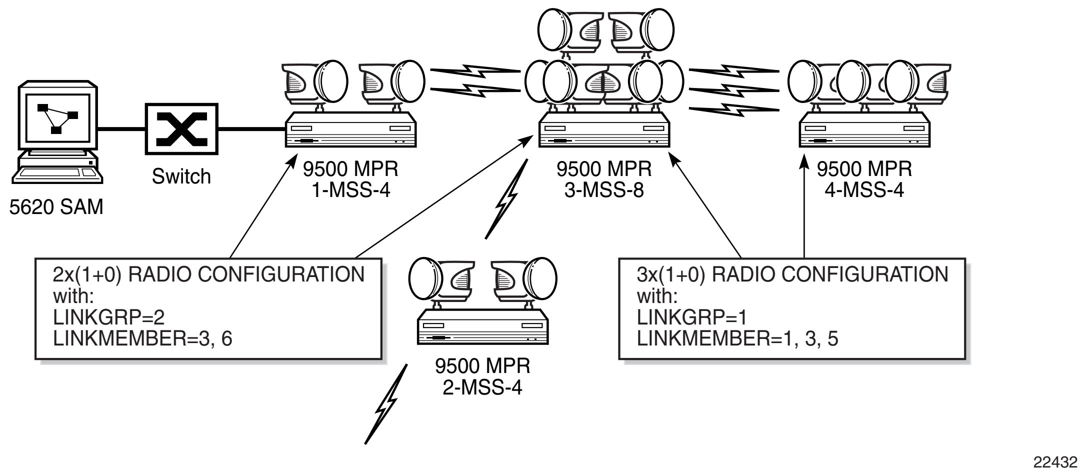


Table 13-1 Connectivity parameter details

	1-MMS-4	2-MSS-4	3-MSS-8	4-MSS-4
2-MSS-4	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (as assigned)	—
3-MSS-8	PPPRF Enabled LinkID (23, 23) PPPRF Disabled LinkID (26, 26)	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (11, 11) PPPRF Disabled LinkID (13, 13) PPPRF Disabled LinkID (15, 15)

To discover multiple radio links, you must provision the radio ports on the 9500 MPR based on the following criteria.

1 Only one radio port can have PPPRF enabled. The far endpoint on the same link must have the same configuration as the first endpoint. PPPRF should be disabled on both endpoints for the second and any subsequent radio links.

2 LinkID requirements include:

   - The LinkID must be enabled for all of the port members of the configuration that have the same LINKGRP, and a different LINKMEMBER that matches the far endpoint.
   - Expected and Sent values must be equal (for example, 11, 11 or 13, 13).
   - For a multiple Nx(1+x) radio configurations on the same node, the LINKGRP must be unique without overlapping (for example, 1 and 2).
   - LinkID should be formatted as LINKGRP:LINKMEMBER in a hexidecimal format where LINKGRP is the first character and LINKMEMBER are the members.
   - Any mismatch between the LinkID at the link level (for example, Send is not equal to Expected) mutes the radio connection (MPT case).

3 As a requirement for the first radio link to be discovered, the remote address must be configured at both endpoints. For subsequent links, alarms cannot be present on the radio port.

4 When Radio Link Aggregation is enabled for any of the radio links between two 9500 MPRs, all radio links must belong to the same LAG.

Configuring user-defined alarms for generic NEs

As part of a generic NE profile, you can map SNMP traps from generic NEs to user-defined 5620 SAM alarms in an alarm catalogue. A generic NE profile can be associated with only one alarm catalogue, but an alarm catalogue can contain up to 150 trap-to-alarm mappings.

A mapping is one of the following types:

- static—A specific SNMP trap is associated with a specific alarm.
- dynamic—The mapping includes one or more transform functions that define alarm properties based on values in SNMP trap PDUs.

Each mapping in a catalogue defines an alarm that the 5620 SAM raises or clears when it receives a specific SNMP trap. A mapping includes standard elements such as the trap OID, alarm type, probable cause, and severity, but can include the following optional elements:

- trap name
- self-clearing designation—specifies that the alarm clears when a specific clearing trap is received, and has the following requirements:
    - If the severity of the raising alarm is a static value, the clearing trap must have a static mapping in the same catalogue as the raising trap, and can be linked to only one raising trap.
    - If the severity of the raising alarm is defined using a transform function, the transform function must include a raising value pair and a clearing value pair.
- FDN extension, which is an alarm-name extension that can include the following:
    - static text
    - scripting functions—expressions that specify the trap PDU values to include; these allow the same alarm type to be raised in response to different traps while uniquely identifying the trap origin in the alarm name.

- additional text—used to provide information of value related to the trap event, for example, troubleshooting actions; the additional text consists of the trap OID by default, but can include the following:
  - static text
  - scripting functions—expressions that specify the trap PDU values to include; these are used to generate a more precise description of the alarm condition
- System Address and/or Interface Index varbind positions for a GNE on which to raise an alarm.

Note — The FDN extension of a generic NE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for generic NE alarms that have FDN extensions, you must filter on the Additional Text field.

A change to an alarm catalogue or to a mapping in a catalogue takes effect when you commit the change.

Transform functions

A transform function is an optional catalogue component that associates one or more values in an SNMP trap PDU with an alarm property such as the alarm name, probable cause, or severity. For example, you can create a transform function that assigns an alarm severity of Critical when the value in a specific varbind is 1, Major when the value is 2, and Minor when the value is 3.

When an alarm mapping includes one or more transform functions, the 5620 SAM can raise multiple alarms in response to the same SNMP trap. A trap value and the associated alarm property value are specified as a value pair in a transform function. You can also specify a default alarm property value that the 5620 SAM assigns to an alarm when a received value is not defined in a value pair.

A transform function defines the input value type, such as integer, and the output alarm property type, such as severity. You can modify these parameters only when the transform function does not contain a value pair and is not used by a mapping.

A transform function returns an empty string when a received value is not defined in a value pair and no default alarm property value is assigned. When the transform function defines the alarm name, probable cause, or severity, the 5620 SAM logs an error in response and does not raise an alarm.

13.3 Workflow to commission and manage devices

The following workflow describes the sequence of high-level tasks required to commission and preconfigure an Alcatel-Lucent device, Telco device, or generic NE for discovery by the 5620 SAM.

1 Using a CLI, enable and configure SNMP on the device.

a See Procedure 13-1 for 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR configuration information.

b See Procedure 13-3 for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco configuration information.

c See Procedure 13-4 for OmniSwitch configuration information.

d See Procedures 13-5, 13-8, and 13-9 for generic NE configuration information.

e See Procedure 13-6 for lightweight generic NE configuration information.

2 If required, enable 5620 SAM management of a 9500 MPR. See Procedure 13-15 for more information.

3 If required, configure the source for 5620 SAM SNMP traps. See Procedure 13-2 for more information.

4 If required, enable the cross launch of a 9400 AWY, MPT-sa, or MSS-1c J-USM manager. See Procedure 13-7 for more information.

5 If required, use a CLI to enable 5620 SAM in-band management of the device by to configure a second trap destination and trap log on the device. See section 13.2 for more information.

Note — Before you configure a discovery rule, as described in chapter 14, you must ensure that a device has routing enabled for the in-band and out-of-band address, as required.

6 If required, establish a route for in-band traffic. For example, to configure a static route or use OSPF. See chapter 30 for more information on static routes. See chapter 31 for more information about OSPF.

7 Configure the 5620 SAM to use in-band, out-of-band, or in-band and out-of-band polling for the device. A 5620 SAM mediation policy specifies the polling interval. See chapter 14 for information about mediation policies.

a See Procedure 13-10 for 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR configuration information.

b See Procedure 13-11 for 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA configuration information.

c See Procedure 13-12 for 7210 SAS configuration information.

d See Procedures 13-5, 13-8, and 13-9 for generic NE configuration information.

e See Procedure 13-13 for 9500 MPR configuration information.

f See Procedure 13-14 for information about editing polling settings for multiple managed devices.

8 If required, configure or modify a generic NE alarm catalogue for use with a generic NE profile. See Procedures 13-16, 13-17, 13-18, 13-19, and 13-20 for more information.

13.4 Alcatel-Lucent and Telco device commissioning procedures

The following procedures describe how to configure Alcatel-Lucent and Telco devices for 5620 SAM management.

Procedure 13-1 To commission a device for 5620 SAM management

This procedure applies to 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR devices. See Procedure 13-3 for information about how to commission a 7250 SAS or Telco device. See Procedure 13-4 for information about how to commission an OmniSwitch device. See the appropriate device documentation for information about using a device CLI.

Caution — Do not apply an SNMP log filter to the 5620 SAM SNMP log. The 5620 SAM cannot manage an NE that has an SNMP log filter applied to the log used by the 5620 SAM, which is typically log ID 98.

1 Open a console window on the device.

2 Enter the following command at the prompt to configure the system address of the device:

configure router interface "system" address *xxx.xxx.xxx.xxx/mask* ↵

where <*xxx.xxx.xxx.xxx*> is the system IP address
mask is the bit mask

3 Enter the following command at the prompt to enable Telnet:

configure system security telnet-server ↵

4 Enter the following command at the prompt to enable FTP:

configure system security ftp-server ↵

5 If required, enter the following command at the prompt to enable SSH2:

configure system security ssh version 2 ↵

6 Enter the following command at the prompt to enable console, FTP, and SNMP access for the appropriate user account on the device:

configure system security user *user_account* access console ftp snmp ↵

where *user_account* is the appropriate user account for Telnet, FTP, and SNMP access, for example, admin

7 If required, enter the following command at the prompt to enable hash encryption for passwords and authentication keys during device configuration save or list operations:

configure system security hash-control read-version *read-version* write-version *write-version* ↵

where

read-version is the version of encryption accepted during read operations, for example, 1, 2, or all to indicate that both are accepted

write-version is the version of encryption used during write operations, for example, 1 or 2

Version 1 encryption uses a simple key algorithm that generates the same character string each time it hashes a specific password or authentication key.

Version 2 encryption uses a more complex key algorithm that generates a different character string each time it hashes a specific password or authentication key.

8 Enter the following commands in sequence at the prompt to set the time zone and time:

configure system time zone *time_zone -offset_from_UCT* ↵

admin set-time *YYYY/MM/DD hh:mm:ss* ↵

where

time_zone is the appropriate time zone, for example, EST

offset_from_UCT is the offset, in hours, from Universal Co-ordinated Time, also known as Greenwich Mean Time, for example, if you specify EST, *offset_from_UCT* is -5, as EST lags UCT by five hours

YYYY/MM/DD hh:mm:ss is the current local time

9 If required, perform one of the following to enable a time protocol.

a Enter the following command at the prompt to enable NTP:

configure system time ntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

b Enter the following command at the prompt to enable SNTP:

configure system time sntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

10 Enter the following commands in sequence at the prompt to enable the SNMPv2 engine and to configure an SNMP community:

configure system snmp no shutdown ↵

configure system snmp packet-size 9216 ↵

configure system security snmp community *community_name* rwa version both ↵

where *community_name* is the SNMPv2 community name

Note 1 — The command is used for the 5620 SAM write mediation policy. If you are using SNMPv2, you must use this mediation policy for read as well, or create another mediation policy that is also configured for rwa.

Note 2 — The SNMPv2 community string name rwa attributes must be enabled for the 5620 SAM to properly manage a node, even if the 5620 SAM is only used to monitor a network.

Note 3 — To configure SNMPv3 management on the device, see Procedure 14-1.

11 Enter the following commands in sequence at the prompt to ensure that the device uses persistent SNMP indexes:

bof persist on ↵

bof save ↵

12 Enter the following commands in sequence at the prompt to save the configuration changes and reboot the device:

admin save ↵

admin synchronize boot-env ↵

admin reboot now ↵

The device initializes with SNMP communication enabled.

13 Type the following to clear the log ID and trap group ID:

configure log ↵

log-id 98 ↵

shutdown ↵

exit ↵

no log-id 98 ↵

no snmp-trap-group 98 ↵

exit all ↵

14 Use a 5620 SAM client to discover the device and to verify that the device configuration allows management of the device, for example, by performing a device configuration backup. See chapter 14 for information about device discovery. See chapter 23 for information about performing device configuration backups.

15 Enter the following commands in sequence at the prompt to ensure that the SNMP trap configuration is correct:

configure log ↵

info ↵

The output should look similar to the following:

```
snmp-trap-group 98
description "5620sam"
trap-target "xxx.xxx.xxx.xxx:162" address
xxx.xxx.xxx.xxx snmpv2c notify-community "privatetrap98"
trap-target "yyy.yyy.yyy.yyy:162" address
yyy.yyy.yyy.yyy snmpv2c notify-community "privatetrap98"
exit
log-id 95
from security
to snmp 1024
exit
snmp-trap-group 95
description "5620sam"
trap-target "xxx.xxx.xxx.xxx:162" address xxx.xxx.xxx.xxx snmpv2c
notify-community "privatetrap98"
trap-target "yyy.yyy.yyy.yyy:162" address  yyy.yyy.yyy.yyy
snmpv2c notify-community "privatetrap98"
exit
```

where

xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server in a standalone 5620 SAM configuration, or one of the two main servers in a redundant configuration

yyy.yyy.yyy.yyy is the IP address of the other 5620 SAM main server in a redundant 5620 SAM configuration, if present

Procedure 13-2 To configure the source for 5620 SAM SNMP traps

If the 5620 SAM is unable to find an SNMP trap target log ID that matches the 5620 SAM configuration log ID, which is by default 98, it recreates the log ID and snmp-trap-group, which results in a single log file that receives traps from two sources.

You can configure the source of log ID 98 by configuring the nms-server.xml file to define the source for traps.

Caution — This procedure requires a restart of the 5620 SAM main and auxiliary servers, which is service-affecting. Ensure that you attempt to perform this procedure only during a scheduled maintenance window.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a text editor.

5 Locate the following text in the file:

```
<snmp

ip="samserverIP"

port="162"

trapLogId="98"
```

where
samserverIP is the IP address of the 5620 SAM main server

This default configuration applies to traps from admin and security.

6 To restrict the source for traps to admin only, add the following line:

```
logIdSourceBits="80"
```

7 Save and close the nms-server.xml file. You must restart the 5620 SAM server for your configuration changes to take effect.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 Enter the following at the prompt to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts.

Note — To prevent a server activity switch in a redundant 5620 SAM system, you must stop the standby 5620 SAM server before you restart the primary main server.

Procedure 13-3 To commission a 7250 SAS or Telco device for 5620 SAM management

This procedure applies to 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices. See Procedure 13-1 for information about how to commission 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR devices. See Procedure 13-4 for information about how to commission an OmniSwitch device. See the appropriate device documentation for more information about using the CLI.

Note — An uncommissioned Telco, 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA device is in Privileged, or enable, mode by default. After you configure an enable mode password for the device in step 6 of this procedure, enable mode is not the default. See the appropriate device documentation for more information about enable mode.

1 Open a console window on the device.

2 Enter the following command to enable further device configuration:

configure terminal ↵

3 Enter the following sequence of commands to set the host name and IP address for the managed device:

hostname *name* ↵

ip address *xxx.xxx.xxx.xxx*/*M* ↵

where
name is the host name
xxx.xxx.xxx.xxx is the IP address
M is the bit mask

Note — Ensure that each 7250 SAS-ES or 7250 SAS-ESA that is going to use in-band management can ping the network interface IP address configured on the 5620 SAM main server; also ensure that the 5620 SAM main server can ping the system IP address of each 7250 SAS-ES or 7250 SAS-ESA.

4 If you are configuring a 7250 SAS-ES or 7250 SAS-ESA, go to step 5. Otherwise, go to step 6.

5 For the 7250 SAS-ES and 7250 SAS-ESA, which support enhanced functionality such as OSPF and VPLS, you must configure a system interface, lo1, so that the 5620 SAM can discover or manage the devices. Enter the following sequence of commands to configure the lo1 system interface:

`interface lo1` ↵

`ip address` ***`xxx.xxx.xxx.xxx`*** **`/32`** ↵

where *xxx.xxx.xxx.xxx* is the IP address

6 Enter the following command to change the switch login password:

`password` ***`password password`*** ↵

where *password* is the new switch login password that is entered twice

7 Enter the following command to set the enable mode password:

`enable password` ***`password password`*** ↵

where *password* is the new enable mode password that is entered twice

8 By default, access ports on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices belong to a default VLAN. The port numbers may differ from those shown in the following examples, depending on which port is designated as the management port. Enter the appropriate sequence of commands to remove the device from the default VLAN.

a For a 7250 SAS, enter the following commands:

`vlan` ↵

`config default` ↵

`remove ports 1/1/2-1/5/4` ↵

`exit` ↵

`exit` ↵

b For a 7250 SAS-ES or 7250 SAS-ESA,enter the following commands:

vlan ↵

config default ↵

remove ports 1/1/2-1/6/2 ↵

exit ↵

exit ↵

c For a Telco device, enter the following commands:

vlan ↵

config default ↵

remove 1/1/1-1/1/# ↵

exit ↵

exit ↵

where # is the number of ports on the card; for example, 24

9 Enter the following command to configure static routes from the device to the 5620 SAM network management domain:

ip route *xxx.xxx.xxx.xxx*/*M* *yyy.yyy.yyy.yyy*

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
M is the 5620 SAM main server subnet mask
yyy.yyy.yyy.yyy is the IP address of the gateway device used to reach the 5620 SAM main server

10 Perform one of the following to configure the required version of SNMP on the device:

a For SNMP v2c:

i Enter the following sequence of commands to configure the SNMP group and users:

snmp-server enable ↵

snmp-server view viewALL 1.3 included ↵

snmp-server group *v2c_group* v2c read viewALL write viewALL notify viewALL ↵

snmp-server user *v2c_user* group *v2c_group* v2c ↵

snmp-server user *v2c_usertrapXX* group *v2c_group* v2c ↵

where

v2c_user is an SNMP user name; for example private. The name must match the SNMP Community String used by the 5620 SAM node discovery mediation policy.

v2c_group is an SNMP trap group name

v2c_usertrapXX is an SNMP trap user name. The name is comprised of the *v2c_user* name followed by trapXX, where XX is a number from 01 to 98. For example, if the *v2c_user* name is private, the *v2c_usertrapXX* name must be privatetrapXX. The name must match the SNMP trap user name used by the 5620 SAM node discovery mediation policy.

ii Enter the following sequence of commands to configure SNMP trap forwarding to the 5620 SAM:

snmp-server target-param *Target v2c_usertrapXX* v2c ↵

snmp-server target-addr *name xxx.xxx.xxx.xxx port# Target* TRAP ↵

snmp-server notify all TRAP ↵

where

Target is a name specified for the SNMP target, for example Target_1

v3_usertrapXX is the user name created in step i above

name is the target name, for example sam

xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server

port# is the SNMP trap receiving port on the 5620 SAM main server; for example, the default of 98 for a standalone or primary main server, or 97 for a standby main server

b For SNMPv3:

i Configure an SNMPv3 user and group.

snmp-server enable ↵

snmp-server view viewALL 1.3 included ↵

snmp-server group *v3_group* v3 priv read viewALL write viewALL notify viewALL ↵

snmp-server user *v3_user* group *v3_group* v3 priv *privpass* auth md5 *authpass*↵

snmp-server user *v3_usertrapXX* group *v3_group* v3 priv *snmppass* auth md5 ↵

where
v3_user is the SNMPv3 user name
v3_group is the name of the SNMPv3 trap group
privpass is the DES privacy encryption password
authpass is the MD5 authentication password
v3_usertrapXX is an SNMP trap user name. The name is comprised of the *v3_user* name followed by trapXX, where XX is a number from 01 to 98. For example, if the *v3_user* name is private, the *v3_usertrapXX* name must be privatetrapXX. The name must match the SNMP trap user name used by the 5620 SAM node discovery mediation policy.

ii Configure SNMPv3 trap forwarding to the 5620 SAM:

snmp-server target-param Target *v3_usertrapXX* v3 priv ↵

snmp-server target-addr *name xxx.xxx.xxx.xxx port# Target* TRAP ↵

snmp-server notify all TRAP

where
Target is the target parameter name, for example Target_1
v3_usertrapXX is the SNMPv3 user name created in i above
name is the target name, for example SAM
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
port# is the SNMP trap-receiving port on the 5620 SAM main server

11 Perform one of the following to configure the STP for a device in a VLAN ring topology:

a Enter the following sequence of commands to configure RSTP:

protocol ↵

rapid-spanning-tree enable ↵

rapid-spanning-tree priority 4096 ↵

b Enter the following sequence of commands to configure MSTP:

protocol ↵

mstp enable ↵

mstp 0 priority 4096 ↵

Note — When you set the MSTP priority, ensure that the devices closest to the 7450 ESS are set with the lowest priority and use instance 0. This enables the STP on all ports. When ports are used for access as SAPs, STP should be disabled.

12 The 5620 SAM supports enhanced functionality such as MPLS LSPs, FRR, and VPLS on the 7250 SAS-ES and 7250 SAS-ESA.

See Table 13-2 to determine what protocol and interface configuration is supported on the 5620 SAM.

Table 13-2 5620 SAM protocol and interface configuration support for the 7250 SAS-ES and 7250 SAS-ESA

Protocols and Interfaces	Description	7250 SAS-ES 2.0	7250 SAS-ES and 7250 SAS-ESA 3.0
Create and configure L3 interfaces	Create L3 interfaces and configure interface properties	CLI	CLI
Configure LDP	Configure LDP on the NE Enter the LDP targeted peers for the NE	CLI	CLI
Configure OSPF	Configure OSPF on the NE, system interface, L3 interfaces, and specified networks	CLI	CLI
Configure OSPF-TE	Configure OSPF-TE on the NE	Not supported	CLI
Configure RSVP	Configure RSVP on the NE, system interface, and L3 interfaces Enable RSVP-TE extensions	CLI	CLI
Configure MPLS	Configure MPLS on the NE, system interface, and L3 interfaces	CLI	CLI
Create and configure MPLS interfaces	Create and configure MPLS interfaces and administrative groups	CLI for MPLS interfaces Administrative groups are not supported	CLI and 5620 SAM

After the devices are configured, perform the following for SNMP v2c.

- Configure a mediation policy that contains a community string user name that matches the one created using CLI, as described in Procedure 14-4.
- Create a discovery rule that represents the devices, and reference the newly created mediation policy, as described in Procedure 14-6.

After the devices are configured, perform the following for SNMPv3.

- Create SNMPv3 users from the 5620 SAM GUI using the NE user configuration manager. See Procedure 21-6 for more information about NE user configuration. Ensure that the following are configured.
    - Give the user SNMP access by enabling the snmp check box.
    - Enter the same User Name as the user name that was created using CLI; for example, *v3_user*
    - On the SNMPv3 tab, select MD5 as the authentication protocol and DES as the privacy protocol.
    - Type the appropriate plain-text ASCII password used as the MD5 authentication key and DES privacy key; for example, *snmppass*.

- Create a new SNMPv3 mediation policy, as described in Procedure 14-4. Ensure that the following are configured:
  - Security Model is SNMP v3 USM
  - SNMP User Name is the same as the user name created using CLI, which is also the name of the NE user configuration created to use SNMPv3.
- Create a discovery rule that represents the devices, and reference the newly created mediation policy, as described in Procedure 14-6.

Procedure 13-4 To commission an OmniSwitch for 5620 SAM management

See the appropriate OmniSwitch documentation for more information about the CLI command syntax and SNMP.

Note 1 — The 5620 SAM cannot discover an OmniSwitch that is configured with the factory default settings.

Note 2 — You must use a direct console port connection to access an OmniSwitch for the first time. All other management methods such as SNMP, Telnet, FTP, and HTTP, are disabled until you enable them.

1 Open a console window using a direct console port connection to the OmniSwitch.

2 Create a Loopback0 interface and assign an IP address to the interface by entering the following at the prompt:

ip interface Loopback0 address *xxx.xxx.xxx.xxx* ↵

where

xxx.xxx.xxx.xxx is the IP address of the interface

Note 1 — Loopback0 is the name assigned to an IP interface to identify an address that is used for network management purposes. The Loopback0 interface is not bound to any VLAN, therefore it always remains operationally active.

Note 2 — The Loopback0 interface name is case-sensitive. Ensure that you enter the name exactly as shown.

3 Enable SNMP sessions on the switch by entering the following at the prompt:

aaa authentication snmp local ↵

4 Enable FTP, Telnet, HTTP, or SSH sessions, if required, by entering the following at the prompt:

aaa authentication ftp local ↵

aaa authentication telnet local ↵

aaa authentication http local ↵

aaa authentication ssh local ↵

5 Perform one of the following to configure the required version of SNMP on the switch and the 5620 SAM:

The OmniSwitch default user, admin, does not have SNMP access. Before the 5620 SAM can discover an OmniSwitch, you must create at least one user on the switch with SNMP access.

a For SNMP v2c:

i Configure an SNMP v2 user by entering the following at the prompt:

`user` ***`user_name`*** **`password`** ***`password`*** **`no auth`** ↵

where
user_name is a username that corresponds to an SNMP v2 user that the 5620 SAM can identify; Alcatel-Lucent recommends that you use the name sam, which is the 5620 SAM default name
password is a password associated with the username; the password is between 8 and 47 characters

Note — If you need to use a different SNMPv2 default user name, use Procedure 6-24 to create an SNMPv2 default user name on the 5620 SAM.

ii Configure SNMP v2 trap forwarding to the 5620 SAM by entering the following at the prompt:

`snmp station` ***`xxx.xxx.xxx.xxx v2 user_name`*** ↵

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username that you created in step i

Trap forwarding configuration occurs automatically when the 5620 SAM discovers a switch and uses the default SNMP v2 user name sam or the user name configured in Procedure 6-24.

iii Configure an SNMP security level that allows the switch to accept all SNMP queries by entering the following at the prompt:

`snmp security no security` ↵

iv Configure an SNMP v2 community string by entering the following at the prompt:

`snmp community map` ***`community_string`*** **`user`** ***`user_name`*** ↵

where
community_string is the name of an SNMP v2 community string that the 5620 SAM can identify
user_name is the SNMP v2 username created in step i

v Create a mediation security policy on the 5620 SAM that uses a community string that matches the string created in step iv. See Procedure 14-4 for information about creating a mediation security policy.

vi Create a discovery rule on the 5620 SAM to discover the switch and reference the policy created in step v. See Procedure 14-6 for information about creating a discovery rule.

b For SNMP v3:

If you need to discover an OmniSwitch using SNMP v3 you must create an SNMP v3 user on the switch that matches an SNMP v3 user defined on the 5620 SAM.

i Configure an SNMP v3 user on the switch by entering the following at the prompt:

user *user_name* password *password* *security_level* ↵

where
user_name is a username that matches an SNMP v3 USM username configured on the 5620 SAM
password is a password associated with the username; the password is between 8 and 47 characters. The password is the plain text ASCII MD5/SHA authentication key and DES privacy key.
security_level is MD5, MD5 + DES, SHA, or SHA + DES

ii Configure SNMP v3 trap forwarding to the 5620 SAM by entering the following at the prompt:

snmp station *xxx.xxx.xxx.xxx* v3 *user_name* ↵

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username created in step i

Trap forwarding occurs automatically when the 5620 SAM discovers a node with a username that matches the SNMP v3 USM username specified in the 5620 SAM mediation policy.

iii Configure the SNMP v3 switch security option that you need by entering the following at the prompt:

snmp security *security_option* ↵

where *security_option* is one of the security options described in Table 13-3

Table 13-3 SNMP security options

Option	Description
no security	All SNMP queries are accepted.
authentication set	Includes: • SNPM v1 and v2 Gets • Non-authenticated v3 Gets and Get-Nexts • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts

(1 of 2)

Option	Description
authentication all	Includes: • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy set	Includes: • Authenticated v3 Gets and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy all (default)	Includes: • Encrypted v3 Sets, Gets, and Get-Nexts
traps only	Includes: • All SNMP requests are rejected

(2 of 2)

iv Create an SNMP v3 user on the 5620 SAM using the NE User Configuration manager. See Procedure 21-6 for information about NE user configuration.

- Enable SNMP to give the SNMP v3 user SNMP access.
- Choose a username that matches the name created on the switch in step i.
- Choose the same SNMP v3 authentication protocol, privacy protocol, and password that is configured on the switch.

v Create an SNMP v3 mediation security policy. See Procedure 14-4 for information about configuring a mediation security policy.

- Choose the SNMP v3 (USM) security model option.
- Choose a username that matches the name created on the switch in step i.

vi Create a discovery rule that uses the mediation security policy created in step v. See Procedure 14-6 for information about creating discovery rules.

6 Use a 5620 SAM client to discover the switch and to verify that the switch configuration allows you to manage the switch.

13.5 Generic NE commissioning procedures

The following procedures describe how to configure the 5620 SAM to manage one or more generic NEs.

Procedure 13-5 To prepare a generic NE for 5620 SAM management using a generic NE profile

Perform this procedure to prepare a non-Alcatel-Lucent device for 5620 SAM discovery and management. See chapter 16 for more information about device management.

Note — For lightweight generic NE management (9400 AWY, MSS-1c, and MPT-sa), see Procedure 13-6.

1 Open a console window on the device. See the appropriate device documentation for information about using the device CLI.

2 Perform the following preconfigurations.

- **i** Enable FTP.
- **ii** Enable Telnet.
- **iii** Enable the SNMP engine.
- **iv** Configure at least one SNMPv1, SNMPv2c, or SNMPv3 community.
- **v** Set the SNMP PDU size to 9216.
- **vi** Enable persistent SNMP indexes.

3 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

4 Click on the Create button and choose Create Generic NE Profile. The Generic NE Profile (Create) form opens.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Generic NE Type
- Generic NE Category
- Sys Object ID
- Description
- Default Element Manager URL
- Chassis MAC Object ID
- Default External EMS
- CLI Supported

Note — You cannot modify the Generic NE Type parameter after the generic NE profile is created; you must delete the generic NE profile and create a profile using the new Generic NE Type parameter value.

6 Click on the CLI Profile tab button and configure the parameters:

- Command Prompt
- Max Number Of Sessions
- Telnet Port
- Pre Login Prompt
- Write Login Prompt
- Write Password Prompt
- Read Login Prompt
- Read Password Prompt
- Error Indicator
- Disable Paging Command
- Reset Command
- Login Timeout (seconds)
- Execution Command Timeout (seconds)
- Login Prompt Optional
- Idle Session Warning Message

7 Configure the following parameters if a login confirmation prompt appears:

- Enable Confirm Prompt
- Prompt
- Answer

The Prompt and Answer parameters are configurable when the Enable Confirm Prompt parameter is selected.

8 Configure the following parameters for a second level of login security, if required:

- Enable Second Login
- Enable Login Command
- Enable Login Prompt

The Enable Login Command and Enable Login Prompt parameters are configurable when the Enable Second Login parameter is selected.

9 Click on the Interface Types tab button to configure an interface for the generic NE.

10 Click on the Add button. The Select Generic NE Interface Type form opens.

11 Configure the filter criteria and click on the Search button. The form displays a list of interface types.

12 Select one or more interface types in the list and click on the OK button. The Select Generic NE Interface Type form closes and the selected interface types are listed on the Generic NE Profile (Create) form.

13 Click on the Routing MIBs tab button. The Generic NE Profile form is displayed.

Note — The Routing MIBs tab button is dimmed if you do not have a valid 5650 CPAM license that has a third-party router quantity greater than zero. See the *5650 CPAM User Guide* for information about 5650 CPAM licenses.

14 Click on the Add button. The Select Generic NE Routing MIB window is displayed.

15 Click on the Search button. A list of the supported Routing MIBs is displayed.

16 Select one or more of the Routing MIBs in the list and click on the OK button. The Select Generic NE Routing MIB window closes. The Generic NE Profile form is displayed.

Note — You must not configure the Routing MIBS and apply the configuration to the Generic NE profile before you configure the interface types. See steps 9 to 12. If you configure the Routing MIBs in the wrong order, you must perform a full node resync and specify the 'ignore time stamp' instruction.

17 Click on the OK button. The Generic NE Profile form reappears with the new generic NE profile.

18 Click on the Apply button.

Note — After you have discovered the NE using the generic NE profile in 5620 SAM, you can use the Routing tree to navigate to and view the discovered routing objects.

19 Click on the Trap Configuration tab button.

Caution — The 5620 SAM assumes that the trap log name on a generic NE is the same as the trap log name on the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, and 7750 SR. Some generic NEs may not support the use of a trap log name that matches the name used by these devices. If this is the case for a generic NE that you need to manage using the 5620 SAM, you may not be able to use the Trap Restoration Logs on the generic NE.

20 Configure the parameters:

- Supports Trap Sequence Number
- Supports Trap Restoration Logs
- Maximum Trap Gap
- Full Node Resync on Max Trap Gap
- Minimum Time Interval Between Full Node Resyncs (seconds)

Caution — The 5620 SAM supports trap sequencing only for devices that increment the trap ID value by 1. Do not enable the Supports Trap Sequence Number parameter if the generic NE increments the trap ID value by anything other than 1.

21 Click on the Select button beside the Script ID parameter in the Trap Configuration Script panel. The Select Script - Generic NE Profile form opens.

The script chosen in this step enables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to manage the generic NE.

Note 1 — A 5620 SAM CLI script to configure the GNE trap destination must already exist before you can select it for use in the generic NE profile. See the *5620 SAM Scripts and Templates Developer Guide* for information on creating CLI scripts.

Note 2 — If the 5620 SAM system is a redundant deployment, ensure that both 5620 SAM main servers are specified in the trap configuration script as SNMP trap destinations to be added.

22 Select a script in the list and click on the OK button. The Select Script - Generic NE Profile form closes and the script identification is displayed on the Generic NE Profile (Edit) form.

23 Click on the Select button beside the Script ID parameter in the Trap De-Configuration Script panel. The Select Script - Generic NE Profile form opens.

The script chosen in this step disables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to unmanage the generic NE.

Note — If the 5620 SAM system is a redundant deployment, ensure that both 5620 SAM main servers are specified in the trap de-configuration script as SNMP trap destinations to be removed.

24 Select a script in the list and click on the OK button. The Select Script - Generic NE Profile form closes and the script identification is displayed on the Generic NE Profile (Edit) form.

25 Click on the Select button beside the Catalogue Name parameter in the Alarm Catalogue panel. The Select Alarm Catalogue - Generic NE Profile form opens.

26 Select an alarm catalogue in the list and click on the OK button. The Select Alarm Catalogue - Generic NE Profile form closes and the catalogue name is displayed on the Generic NE Profile (Edit) form.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button. The Generic NE Profile (Edit) form closes.

29 Close the Generic NE Manager form.

Procedure 13-6 To prepare a lightweight generic NE for 5620 SAM management using a generic NE profile

Perform this procedure to prepare a lightweight (9400 AWY, MSS-1c, and MPT-sa) device for 5620 SAM discovery and management. See chapter 16 for more information about device management.

Note — An MPT-sa/MPRe is an MPT-MC/MPT-HC in standalone mode.

1 Before managing the MPT-sa/MSS1c/AWY, the 5620 SAM IP address must be registered with any NEs that are to be managed as lightweight generic NEs. To register the 5620 SAM IP address perform the following steps.

i Open MCT or Multi-version NEtO and open the required NE, MPRe/MSS1c/AWY.

ii Use the Trusted SNMP Manager option in the navigation tree to register the 5620 SAM IP address.

iii Enter 162 as the Traps UDP Port for the MPT-sa/MSS1c/AWY.

iv Enter Network Manager Layer as the Type.

v Once the 5620 SAM IP address is registered, close the MCT tool.

2 Perform the following steps to ensure that the SystemGneProfilesNames flag is set correctly in the nms-server.xml file for lightweight generic NE management of 9400 AWY, MSS-1c, or MPT-sa.

Note — To create a lightweight managed NEs profile, the user does not have to enter any parameters such as SysObject ID. After completion, the respective profile is the default profile in the 5620 SAM.

i Go to directory /opt/5620sam/server/nms/config.

ii Open the nms-server.xml file.

iii Go to the line systemGNEProfileNames=“ ”

iv Edit as systemGNEProfileNames=“MPTSA” or systemGNEProfileNames=“MSS1c” or systemGNEProfileNames=“9400AWY” or systemGNEProfileNames=“MPTSA, MSS1c, 9400AWY”

v Save and close the file.

vi Go to path /opt/5620sam/server/nms/bin

vii Execute the following command:

su samadmin nmsserver.bash read_config ↵

viii Using Discovery Manager, manage the MPT-sa/MSS1c/AWY with the default setting for snmpv2 as read-write access policy. Configure the community string as “SNMP-trap” for trap access mediation policy.

ix Observe that a new group has been created in the Equipment Network tree and that all related generic NEs are located in this group.

3 To auto-populate the alarms catalogue, follow the steps below:

Note 1 — To see the alarms from MPRe/MSS1c/AWY the user does not need to do any manual mapping from the Trap ID to the Alarm Name. Follow the steps below to display the automatic binding of known traps reported in 5620 SAM.

Note 2 — AFter the alarm catalogue is auto-populated, the alarms for which the 5620 SAM receives traps are processed. Existing alarms on the Generic NE are not processed.

i Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

ii Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.

iii Select the created generic NE profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

iv Click on the More Actions button and choose Populate Alarm Catalogue from the drop-down. The respective Alarm catalogue is created.

v Click on the Trap Configuration tab button. Attach the Alarm catalogue to the respective profile.

vi Click on the Interface tab button. Add each of the respective interfaces or all interfaces to get the traps. All alarms should now be visible in your 5620 SAM client.

vii Generate new alarms from MPRe/MSS1c/AWY, the alarms are displayed in the 5620 SAM alarm window.

Procedure 13-7 To cross launch the 9400 AWY, MPT-sa, or MSS-1c J-USM manager

Perform this procedure to enable the cross launch of a Java-based EMS/craft terminal.

1 Perform Procedure 13-5 to discover the 9400 AWY, MPT-sa, or MSS-1c GNE.

2 Perform one of the following steps to specify the NEtO directory path:

Note — Option B is the preferred method.

a To specify the NEtO directory path for every node:

i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

ii Right-click on the 9400 AWY, MPT-sa, or MSS-1c GNE in the Equipment view and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

iii Specify the directory name in the External EMS field.

b To configure and use the same NEtO directory path for all nodes that are discovered using a discovery rule:

i Open the Discovery Manager window and choose the Discovery Rules tab button.

ii Select the existing Discovery Rule that was created for all the nodes and select the Properties button, the Topology Discovery Rule [Edit] form opens with the General tab button displayed.

iii Specify the NEtO directory name in the Default External EMS field

Note — To cross launch a 9400 AWY NE, retain the NEtO software directory in your 5620 SAM client and remove any space in the NEtO directory description, for example, C:\9500SAM\8.0\NEtOETSI\multiversion2.1\NEtO_MultiVersion\NEtO.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The Network Element (Edit) form closes.

5 Right-click on the GNE and choose External Element Manager from the contextual menu. The MCT/NEtO is launched.

Procedure 13-8 To modify a generic NE profile

Perform this procedure to change the parameters in an existing generic NE profile.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.

3 Select a generic NE profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

The following tabs contain configurable parameters:

- General—contains parameters that identify the generic NE type
- CLI Profile—contains parameters that define the console window prompts and commands
- Trap Configuration—contains parameters that define the SNMP trap management configuration
- Interface Types—allows the association of multiple types of interfaces with the generic NE profile. A generic NE interface is selectable as the endpoint of a 5620 SAM physical link.

4 Modify the parameters for the generic NE profile, as required.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Generic NE Profile (Edit) form closes.

7 Close the Generic NE Manager form.

8 If you modify the list of interfaces on the Interface Types tab, perform the following steps.

Caution — If you modify the list of interfaces on the Interface Types tab, you must resynchronize the entire generic NE without comparing timestamps to ensure that the 5620 SAM database is correctly updated with the new interface information.

i Right-click on the generic NE in the 5620 SAM topology map and choose Resync from the contextual menu. The Resync Site(s) form opens with the Resync Options panel displayed.

ii Click on the Next button. The Force Resync panel is displayed.

iii Select the Ignore Timestamps parameter.

iv Click on the Finish button. The 5620 SAM resynchronizes the generic NE.

v Close the Resync Site(s) form.

Procedure 13-9 To delete a generic NE profile

Note 1 — You cannot delete a generic NE profile that is associated with a managed generic NE. You must unmanage the generic NEs associated with a generic NE profile before you can delete the profile.

Note 2 — You cannot delete a generic NE profile when a generic NE associated with the profile is a target of a CLI script. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1. Unmanage and delete the generic NEs that are managed using the generic NE profile. See chapter 14 for more information.
2. Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.
3. Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.
4. Select a profile in the list and click on the Delete button. A dialog box appears.
5. Click on the Yes button. The 5620 SAM deletes the generic NE profile.
6. Close the Generic NE Manager form.

13.6 Device management procedures

The following procedures describe how to configure device management.

Procedure 13-10 To configure polling for a 7450 ESS, 7705 SAR, 7710 SR, or 7750 SR

1. Choose Equipment or Routing from the drop-down menu on the navigation tree.
2. Open the Network icon. The managed devices are displayed.
3. Click on an icon that represents a 7750 SR, 7450 ESS, 7710 SR or 7705 SAR.
4. Right-click and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
5. Record the system IP address and the management IP address. Configure the Location and OLC State parameters, if required.
6. Click on the Polling tab button.
7. Click on the General tab button.
8. Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 14-4 for more information.
9. Configure the Redundant Synchronization Mode parameter.

10 Verify that the Persistent SNMP Indices parameter is set to true to ensure persistent SNMP indices are used.

11 Configure the parameters:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain
- Separate LI Administration
- LI Local Save Allowed

Note 1 — To configure LI parameters, you require LI user privileges.

Note 2 — To view LI configuration information, you need LI privileges. Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu, and click on the LI Configuration Status tab button.

12 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

13 Click on the Management tab button.

14 Configure the following parameters to specify an L3 management interface for in-band management, if required:

- L3 Management Interface
- Enable L3 Management Interface

15 Configure the following parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection
- Primary Route Preference
- Secondary Route Preference

Note 1 — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred or In Band Preferred.

Note 2 — To avoid a communications outage between the 5620 SAM and managed NEs, the parameter settings in the Management Preference panel must match the parameter settings in the Notifications Preferred Management panel. See the Management IP Selection parameter description for more information.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 13-11 To configure polling for a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA

1 Choose Equipment or Routing from the drop-down menu on the navigation tree.

2 Open the Network icon. The managed devices are displayed.

3 Click on an icon that represents a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA.

4 Right-click and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

5 Record the system IP address and the management IP address. Configure the Location and OLC State parameters, if required.

6 Click on the Polling tab button.

7 Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 14-4 for more information.

8 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 13-12 To configure polling for a 7210 SAS

Perform this procedure to configure polling policies for a 7210 SAS-D 6F 4T, 7210 SAS-D 6F 4T ETR, 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP device.

1 Choose Equipment or Routing from the drop-down menu on the navigation tree.

2 Open the Network icon. The managed devices are displayed.

3 Click on the device icon.

4 Right-click on the icon and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

5 Record the system IP address and the management IP address. Configure the Location and OLC State parameters, if required.

6 Click on the Polling tab button.

7 Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 14-4 for more information.

8 Verify that the Persistent SNMP Indices parameter is set to true to ensure that persistent SNMP indices are used.

9 Configure the parameters in the Bof Configuration panel, if required:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain

10 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

11 Click on the Management tab button.

12 On the In Band panel, configure the parameters:

- L3 Management Interface
- Enable L3 Management Interface

13 On the Management Preference panel, configure the parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection

Note 1 — The Active Management IP, Auto Revert to Preferred, and Management IP Selection parameters are configurable only on the 7210 SAS-D 6F 4T and 7210 SAS-D 6F 4T ETR, Release 3.0 or later, the 7210 SAS-E, Release 2.0 R2 or later, and the 7210 SAS-M, Release 2.0 R2 or later. The 7210 SAS-X Release 3.0R2 or later supports a Management IP Selection value of Out of Band Preferred.

Note 2 — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred, In Band Preferred, or In Band Only.

14 On the Notifications Preferred panel, configure the following parameters:

- Primary Route Preference
- Secondary Route Preference

15 You can configure two uplinks in the BOF for port redundancy. If the image path and configuration file path are local, you do not need to configure the IP address and routing information for uplink A and uplink B. You can optionally obtain IP parameters using DHCP when you configure a value of 0 for the uplink port IP address. The DHCP server should be configured to provide the IP address and the default gateway information that is used to reach the server where the image and configuration files are stored.

16 Click on the 7210 BOF tab button and on the Select button in the Uplink A panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

17 Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink A panel.

18 Configure the following parameters in the Uplink A panel:

- IP Address
- Mask
- VLAN ID

19 Click on the Select button in the Uplink B panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

20 Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink B panel.

21 Configure the following parameters in the Uplink B panel:

- IP Address
- Mask
- VLAN ID

22 Click on the Uplink Routes tab button and on the Create button. The Uplink Route Configuration (Create) form opens.

23 Configure the following parameters:

- Uplink
- Route Destination
- Mask
- Next Hop

24 Click on the Apply button if you need to add more than one uplink route or the OK button if you only need to add one route. A dialog box appears.

25 Click on OK to save your configuration.

26 Repeat steps 23 to 25 to add another uplink route. You can add up to ten routes for each uplink.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 13-13 To configure polling for a 9500 MPR

1 Choose Equipment or Routing from the drop-down menu on the navigation tree.

2 Open the Network icon. The managed devices are displayed.

3 Click on an icon that represents a 9500 MPR.

4 Right-click and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

5 Record the system IP address and the management IP address. Configure the Location and OLC State parameters, if required.

6 Click on the Polling tab button.

7 Configure the Scheduled Polling parameter if you are configuring a 9500 MPR. Scheduled polling is configured using the Mediation configuration form. See Procedure 14-4 for more information.

8 View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 13-14 To edit polling settings for multiple devices

You can use the list of managed devices from the Discovery Manager Resync Status tab to modify polling settings for a device or devices; for example, when you want to enable or disable polling on numerous managed devices.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens.

2 Click on the Resync Status tab button.

3 Select a device or devices from the list.

4 Click on the Properties button. When you choose multiple devices, the Network Element (Multiple Instances) (Edit) form opens.

You can only configure those parameters that are common to all devices selected from the list.

5 Click on the Polling tab button.

6 Enable or disable polling using the Scheduled Polling parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 13-15 To enable 5620 SAM management of a 9500 MPR

Perform this procedure to enable the 5620 SAM to manage the 9500 MPR and to allow NEtO sessions to be opened using the 5620 SAM GUI.

You must first install the NEtO software on a 5620 SAM client station and modify the client configuration. See the 9500 MPR user documentation for more information about how to install and use the NEtO software. See Procedure 17-14 for information about how to start NEtO from the 5620 SAM GUI.

1 Log in to a 5620 SAM client station.

2 Perform Procedure 14-6 to create a discovery rule for the device.

3 Discover a 9500 MPR NE and verify that the 5620 SAM can manage the device.

Note — The 5620 SAM server and NEtO cannot be run on the same machine. The 5620 SAM client and NEtO (not the 5620 SAM Server) must be on the same machine.

4 On a Windows client, navigate to the 5620 SAM client path *\5620sam\client\nms\thirdparty\config* directory.

5 Open the one the following 9500 MPR property files using a plain-text editor:

- Alcatel-MPR-9500_3.3.0.properties is for A/E-3.3
- Alcatel-MPR-9500_3.2.0.properties is for A/E-3.2
- Alcatel-MPR-9500_3.1.0.properties is for A/E-3.1
- Alcatel-MPR-9500_3.0.0.properties is for 3.0
- Alcatel-MPR-9500_1.0.0.properties id for older releases (example, A-2.2.1, A-2.2.0, A-1.2, E-1.4, E-1.3, E-2.1)

6 Edit the NEtO directory path in the variable *install_dir =${path}*.

For example for a Windows client, the paths could be:

- *install_dir=D:\\NEtO*
- *install_dir=C://9500MPR//MPRE_CT_V01.22.01*, or
- *install_dir=D:\\NM\\SAM\\NEtO_Multiversion\\NEtO*

7 As required, edit the profile name. The format is, profile_name = <role> <community string> <user id> <password>. For example, profile_name = admin private initial adminadmin.

Note — If you do not edit the profile name, the community string is derived from the mediation policy of the discovery rule .

8 Save and close the file.

9 Select the equipment view of the navigation tree on the 5620 SAM GUI. Right-click on a 9500 MPR NE, and select External Element Manager from the menu.

10 Verify that the NEtO software launches.

Procedure 13-16 To create a generic NE alarm catalogue

Perform this procedure to create an alarm catalogue for use with a generic NE profile.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Click on the Create button and choose Create Generic NE Alarm Catalogue. The Generic NE Alarm Catalogue (Create) form opens.

3 Configure the parameters:

- Catalogue Name
- Description
- Version

4 Perform Procedure 13-17 to create a transform function for the catalogue, if required.

5 Click on the Mappings tab button.

6 Click on the Create button to create a raising alarm mapping. The Generic NE Alarm Mapping (Create) form opens.

7 Configure the following parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text

8 Perform one of the following using the parameters in the Alarm Name panel.

a Specify a static alarm name by configuring the Alarm Name parameter.

b Specify a dynamic alarm name. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

9 Perform one of the following using the parameters in the Probable Cause panel.

a Specify a static probable cause. Perform the following steps.

i Click on the Select button beside the Probable Cause parameter. The Select Property form opens with a list of probable causes displayed.

ii Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping (Create) form.

b Specify a dynamic probable cause. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

10 Perform one of the following using the parameters in the Severity panel.

a Specify a static severity by configuring the Severity parameter.

b Specify a dynamic severity. Perform the following steps.

Note — When you specify the use of a transform function for the alarm severity, the Mapping Type changes to Raising/Clearing. You cannot create a clearing mapping for this type of mapping; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

11 Configure the varbind positions for specific objects on a GNE in the Alarmed Object panel:

- System Address Varbind Position
- Interface Index Varbind Position

Note — In order to configure the System Address Varbind Position and Interface Index Varbind Position parameters, you must set the Alarm Name parameter to GNE MTIE Alarm.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

14 Repeat steps 6 to 13 to create an additional raising alarm mapping, if required.

15 If you do not need to create a clearing alarm mapping, go to step 25.

16 To create a clearing alarm mapping, select a raising alarm mapping in the list and click on the Create Clearing button. The Generic NE Alarm Mapping (Create) form opens.

Note 1 — A raising alarm mapping is indicated by the word Raising in the Mapping Type list column.

Note 2 — You can create a clearing alarm mapping only when the corresponding raising alarm is in the same alarm catalogue.

Note 3 — You can associate a clearing alarm mapping with only one raising alarm mapping.

Note 4 — You cannot create a clearing mapping for a mapping that uses a transform function to define the alarm severity; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

17 Configure the parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text

Note 1 — A static clearing alarm mapping inherits the following values from the associated raising alarm:

- Alarm Name
  This value must match the raising alarm value.
- Probable Cause
  This value must match the raising alarm value.
- FDN Extension
  The resulting text string must match the text string generated by the raising mapping.
- Additional Text
  The resulting text string must match the text string generated by the raising mapping.

See Procedure 13-19 for information about modifying the Alarm Name or Probable Cause value.

Note 2 — The explicit FDN Extension and Additional Text values can differ from the values in the raising mapping, but the generated text strings must match. For example, if the object name is in varbind 2 of the raising trap and in varbind 3 of the clearing trap, the parameter values name different varbinds but the script output is identical.

Note 3 — The alarm severity in a clearing alarm mapping is set to Cleared and cannot be changed.

18 Perform the following steps to specify a dynamic alarm name, if required, using the parameters in the Alarm Name panel.

- **i** Select the Specify Transform Function parameter.
- **ii** Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.
- **iii** Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.
- **iv** Configure the Varbind Position parameter.

19 Perform the following steps to specify a dynamic probable cause, if required, using the parameters in the Probable Cause panel.

- **i** Select the Specify Transform Function parameter.
- **ii** Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.
- **iii** Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.
- **iv** Configure the Varbind Position parameter.

20 Click on the OK button. A dialog box appears.

21 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

22 Repeat steps 16 to 21 to create and additional clearing alarm mapping, if required.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The Generic NE Alarm Mapping (Edit) form closes.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes.

27 Close the Generic NE Manager form.

Procedure 13-17 To create a transform function for a generic NE alarm catalogue

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Click on the Create button and choose Create Generic NE Alarm Catalogue. The Generic NE Alarm Catalogue (Create) form opens.

3 Click on the Transform Functions tab button.

4 Click on the Create button. The Generic NE Alarm Transform Function (Create) form opens.

5 Configure the parameters:

- Transform Function Name
- Out Value Type
- Specify Default Out Value

6 If you enable the Specify Default Out Value parameter, click on the Select button beside the Default Out Value parameter. The Select Property form opens. Otherwise, go to step 8.

7 Select a value in the list and click on the OK button. The Select Property form closes, and the value is displayed on the Generic NE Alarm Transform Function (Create) form.

8 Click on the Pairs tab button.

9 Click on the Create button. The Pair (Create) form opens.

10 Configure the In Value parameter.

11 Click on the Select button beside the Out Value parameter. The Select Property form opens.

12 Select a value in the list and click on the OK button. The value is displayed on the Pair (Create) form.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Pair (Create) form closes, and the value pair is listed on the Generic NE Alarm Transform Function (Create) form.

15 Repeat steps 9 to 14 to add another value pair, if required.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Generic NE Alarm Transform Function (Create) form closes, and the transform function is listed on the Generic NE Alarm Catalogue (Edit) form.

18 Repeat steps 4 to 17 to create another transform function, if required.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes.

21 Close the Generic NE Manager form.

Procedure 13-18 To add an alarm mapping to a generic NE alarm catalogue

Note — A modification to a generic NE alarm catalogue takes effect when you commit the change.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Configure the Description and Version parameters, if required.

5 Perform steps 4 to 27 in Procedure 13-16.

Procedure 13-19 To modify or delete a generic NE alarm mapping

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Mappings tab button.

5 Perform one of the following.

a Modify the mapping. Perform the following steps.

Note — A modification to a generic NE alarm mapping takes effect immediately after you commit the change.

i Select a mapping in the list and click on the Properties button.The Generic NE Alarm Mapping (Edit) form opens.

Note — To change the Alarm Name value in a raising alarm mapping and in the associated clearing alarm mapping, you must do one of the following:

- Configure the parameter in each mapping simultaneously by selecting both mappings before you click on the Properties button.
- Configure the parameter in one mapping at a time and commit the changes to the catalogue only after both mappings are modified.

ii Configure the following parameters:

- Trap Name
- Administrative State
- Alarm Name
- Severity
- FDN Extension
- Additional Text
- Use Default Additional Text

iii Click on the Select button beside the Probable Cause parameter. The Select Property - Generic NE Alarm Mapping form opens with a list of probable causes displayed.

iv Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Generic NE Alarm Mapping (Create) form closes.

b Delete the mapping. Perform the following steps.

Note — When you delete a generic NE raising alarm mapping, the associated clearing mapping is also deleted.

i Select a mapping in the list and click on the Delete button. A dialog box appears.

ii Click on the OK button. The 5620 SAM deletes the generic NE alarm mapping.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes, and the Generic NE Manager form reappears.

8 Close the Generic NE Manager form.

Procedure 13-20 To delete a generic NE alarm catalogue

Note 1 — You cannot delete an alarm catalogue that is associated with a generic NE profile. You must remove the alarm catalogue from each associated generic NE profile before you can delete the catalogue.

Note 2 — When you delete a generic NE alarm catalogue, you delete the alarm mappings that the catalogue contains.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Generic NE Profiles tab button. The tab lists the generic NE profiles to which the alarm catalogue is assigned.

5 If no profiles are listed, go to step 8.

6 Perform the following steps to remove a profile association.

- **i** Select a profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.
- **ii** Click on the Trap Configuration tab button.
- **iii** Click on the Clear button in the Alarm Catalogue panel. The Catalogue Name value is removed from the form.
- **iv** Click on the OK button. A dialog box appears.
- **v** Click on the Yes button. The Generic NE Profile (Edit) form closes, and the Generic NE Alarm Catalogue (Edit) form reappears.

7 Repeat step 6 for each listed profile.

8 Close the Generic NE Alarm Catalogue (Edit) form. The Generic NE Manager form reappears.

9 Select the alarm catalogue in the list and click on the Delete button. A dialog box appears.

10 Click on the Yes button. The 5620 SAM deletes the generic NE alarm catalogue.

11 Close the Generic NE Manager form.

14 — Device discovery

14.1 Device discovery overview

The 5620 SAM simplifies network provisioning by discovering NEs and reconciling their properties with the contents of the 5620 SAM database.

The 5620 SAM discovers NEs using SNMP. During the discovery process, the 5620 SAM scans the network for devices according to user-specified IP addresses or IP address ranges. When the IP address used to discover a device is the system IP address, also called the system ID, management is considered in-band. When the IP address used to discover the device is the management IP address of the device management port, management is considered out-of-band. See chapter 13 for more information about in-band and out-of-band management.

After the 5620 SAM discovers a device, it sets the device state to Managed and adds the device properties to the 5620 SAM database. To discover one or more devices, you use the 5620 SAM Discovery Manager to create discovery rules and scan the network as specified by the rules.

Discovery rules contain rule elements that specify which devices or subnets are to be included in or excluded from the discovery process. A discovery rule can contain multiple rule elements. For example, you can configure one rule element to discover a subnet and another to exclude specific IP addresses from the subnet.

Note — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on an NE, for example, using a CLI.

SNMP management

Simple Network Management Protocol, or SNMP, is an application-layer protocol that provides a message format to facilitate communication between SNMP managers and agents. SNMP provides a standard framework for NE monitoring and management from a central location.

An SNMP manager controls and monitors the activities of network hosts that use SNMP. An SNMP manager uses a get operation to obtain a value from an SNMP agent, and uses a set operation to store a value in the agent. The manager uses definitions from a management information base, or MIB, to perform operations on the managed device, for example, retrieving data values, replying to requests, and processing SNMP notifications called traps.

SNMPv1 and SNMPv2c provide no security, authentication, or encryption. Without authentication, an unauthorized user is able to perform SNMP network management functions and eavesdrop on management information as it passes from one system to another.

SNMPv3 requires that an authentication and encryption method such as SSH is assigned to each user for validation by the NE. SNMPv3 authentication and encryption enable an NE to validate the system that issues an SNMP message and to determine whether another system has tampered with the message.

For information about device-specific SNMP support, see the SNMP chapter of the appropriate *System Management Guide* for the device. For information about SSH security, see section 14.4.

IPv6 discovery

The 5620 SAM supports the discovery of devices that use IPv6 in-band or out-of-band management IP addresses. In order for the 5620 SAM to discover and manage a device that uses IPv6, the device must have an IPv6 address on the management port, system interface, or both. The 5620 SAM main server must also be given an IPv6 address during installation.

Note — To manage 7750 SR, 7710 SR, or 7450 ESS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

The IP version that the 5620 SAM uses to discover a device is specified in each discovery rule. If the 5620 SAM discovers both IPv4 and IPv6 addresses on the system interface of a device, it discovers the device using the address that corresponds to the IP version specified in the discovery rule.

Discovery and SNMP packet size

Each 5620 SAM-managed device must be configured to send SNMP packets of up to 9216 bytes in size. You must ensure that each device between the managed devices and the 5620 SAM can handle an MTU size of 9216 bytes, or is configured to forward fragmented SNMP packets.

Consider the following:

- When an intermediate network device receives SNMP traffic, it must be able to process packets of up to 9216 bytes in size. If this exceeds the MTU size of the intermediate device, and the device cannot forward fragmented packets, the packets may be dropped and device discovery may fail.
- Verify that large packets can travel from the managed devices to the 5620 SAM by using CLI to ping the IP address of the 5620 SAM main server using a large packet. See the *5620 SAM Troubleshooting Guide* server troubleshooting chapter for more information about using traceroute and ping to verify packet transport.

Unmanaging or deleting devices

Using the 5620 SAM to unmanage a device excludes the device from the managed network, but a reference to the device remains in the 5620 SAM discovery system. The unmanage function may be used for unusual conditions such as when the 5620 SAM requires a complete refresh of NE data because of data corruption. Unmanaging a device results in a loss of management data for the selected device, which includes, but is not limited to, the following:

- object names and descriptions
- statistics
- alarms
- physical links
- policies
- script results
- scheduled activities
- NE backups

Deleting a device results in the complete loss of management data for the device and completely removes the device from the managed network.

Caution — If you use the 5670 RAM to process 5620 SAM statistics, unmanaging or deleting an NE results in the loss of all historical 5670 RAM AA statistics for the device.

14.2 Resynchronization of NEs

Full Resync status is independent from partial resync and reachability status, it only provides the status of the last full resync.

There are three resync status related attributes on the NE:

- Resync Status,
- Last Resync Start Time
- Last Resync End Time

These attributes are only updated if the resync operation is a full resync or a scheduled resync. These attributes will not be updated by a partial resync.

The Resync status is displayed in the Resync Status column in the Resync tab. See Procedure 14-6 for more information.

- Full Resync Done indicates that the 5620 SAM resynchronized with all or a subset of the MIB entry tables for an NE.
- Full Resync Failed indicates that the attempt of the 5620 SAM to resynchronize with all or a subset of the MIB entry tables for an NE failed.

  A failed status does not indicate that the SNMP agent on the managed device is not reachable. If the agent is unreachable, an SnmpReachabilityProblem alarm is raised against the managed device and the node icon is red. When the agent becomes reachable, the alarm is cleared.
- Requested indicates that the resynchronization request has entered the request queue.

14.3 Mediation and SNMP MIBs

A 5620 SAM mediation policy defines the interval at which the 5620 SAM polls NEs for SNMP MIB configuration changes. You can use the Mediation and MIB Entry Policy forms to view the information in an SNMP MIB. See Procedure 14-4 for more information.

You can use the 5620 SAM client GUI to list the contents of the device MIBs that the current 5620 SAM system supports. The list includes the following information:

- the MIB name
- the MIB version; the 5620 SAM software may support multiple MIB versions
- the OID of a MIB entry
- the MIB entry name
- the 5620 SAM polling interval for a MIB or MIB entry

See Procedure 14-21 for information about listing and saving SNMP MIB information.

14.4 SSH security

SSH is a protocol that provides secure file transfer and file system access between the 5620 SAM, and managed NEs. SSH version 2, or SSH2, is enabled by default on the following device types:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

SSH2 supports the use of public/private encryption-key pairs to perform authentication based on public key cryptography. A public/private key pair is generated on an NE. The private key is stored locally on the NE, and the public key is specific to SSH2 clients and persists in the 5620 SAM for future communication with the SSH2 server on the NE. The public key is used to verify that the client is connecting to the correct SSH2 server.

An SSH2 server identifies itself to a client by sending a message that is signed with the private key of the server. The 5620 SAM uses the public key of the SSH2 server to authenticate the identity of the server.

SSH2 host key management

An NE sends an SSH2 host key on the first attempt of the 5620 SAM to make an SSH2 connection. The 5620 SAM automatically accepts the public key fingerprint and stores it locally. After the first connection, the local copy of the fingerprint is used for server authentication during subsequent sessions.

If a different host key is sent by the same NE in a subsequent session, the connection is rejected and the 5620 SAM raises an alarm. If the user verifies that the host key of the SSH2 NE has been changed in a legitimate manner, for example, when the SSH server is rebooted and host key persistence is not configured, the user can manually accept the key by removing the mismatched host key entry from the SSH2 known host manager of the 5620 SAM. This removes the SSH2 fingerprint from the 5620 SAM database. Connections are then accepted from the NE until the SSH server is again rebooted.

Note — By default, SSH host keys do not persist in the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X24F2XFP, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

Host keys always persist in the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA.

Alcatel-Lucent recommends that you configure the host key persistence on an SSH2 NE to retain the public key fingerprint across reboots. If public key persistence is not enabled, a 5620 SAM operator must manually accept a new key and remove an alarm each time a connection attempt is made after the NE reboots.

SSH2 and NE CLI sessions

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 instead of Telnet is used for each CLI session. The following devices support SSH2 CLI sessions:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- generic NE

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and script management

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 is used instead of Telnet for each script execution session. The following devices support the use of SSH2 for management using the 5620 SAM Script Manager:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- generic NE

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and secure file transfers

When secure file transfers are specified in the mediation policy of an SSH2-capable device, SCP is used instead of FTP for backups, restores, software upgrades, and statistics collection. The following devices support the use of SSH2 for secure file transfers:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6850E
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E

SSH and device management

The 5620 SAM supports the management of 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA devices using CLI. When the mediation policy for a device is configured to use SSH2, secure CLI communication is used to manage the device. Table 14-1 lists different SSH protocols and the compatibility of each with different device types.

Table 14-1 SSH2 and NE compatibility

Protocol	7210 SAS-M 24F 7210 SAS-M 24F 2XFP 7210 SAS-M 24F 2XFP ETR 7210 SAS-X 24F 2XFP 7450 ESS 7705 SAR 7710 SR 7750 SR	7250 SAS 7250 SAS-ES 7250 SAS-ESA	Generic NE
SSH2	✓	✓	✓
SCP	✓		
Device management using SSH2		✓	

Note — SSH2 communication with a device may be slower to establish than other types of communication because of the encryption and authentication computations that are required.

14.5 Server resource management

The 5620 SAM supports the grouping of NEs by network function for increased SNMP mediation efficiency.

Resource allocation is automatically configured during 5620 SAM installation and network discovery based on the available system resources, and the numbers and types of NEs that are to be managed. The resource group to which an NE belongs is initially determined by the device type. The following are the 5620 SAM NE resource groups and the default device assignments:

- global—for 5620 SAM tasks that are not associated with NEs
- default—for NEs that do not belong to a specific resource group
- core—for 7450 ESS and 7750 SR devices
- middle—for 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7710 SR, and 7705 SAR devices
- edge—for 7250 SAS, Telco, and similar devices
- GNE—for other network devices

The 5620 SAM logs the system load of each resource group at regular intervals. An Alcatel-Lucent support representative can monitor system resource usage, determine whether the current resource allocation is appropriate, and reconfigure resource management, if required.

Caution — Only a qualified Alcatel-Lucent support representative can assess or configure 5620 SAM server resource management. Contact Alcatel-Lucent technical support for more information.

14.6 SNMP event notification policies

To reduce the 5620 SAM processing load associated with SNMP events, you can configure a policy that specifies which SNMP traps the 5620 SAM processes. An event notification policy acts as a filter that enables or disables the processing of specific SNMP traps for a specific NE type and version.

A 5620 SAM operator with an admin or operations scope of command role and write access permission to the policy package can create an event notification policy using the Mediation form. The 5620 SAM assigns a default event notification policy to an NE during initial device discovery. A 5620 SAM operator can create and apply a policy that specifies which traps to process and which to ignore. 5620 SAM processing is enabled for all supported traps in the default policy. See Procedure 14-7 for more information about configuring an event notification policy.

The following conditions apply to event notification policies:

- After an NE upgrade, the 5620 SAM processes the new traps generated by the upgraded NE. A 5620 SAM administrator must ensure that the event notification policies that are in effect before an NE upgrade are correctly configured, and must modify them after the upgrade to silenced new traps, if required.
- 5620 SAM software upgrades do not affect existing event notification policies.

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

SNMP statistics that include the number of ignored traps for an NE are available from the Statistics tab of the NE properties form.

14.7 Workflow for device discovery

The following workflow describes the sequence of high-level tasks required to discover network devices. The following are required must be true before the 5620 SAM can discover a device:

- Each Alcatel-Lucent or Telco device is commissioned; see chapter 13 for commissioning information.
- Each non-Alcatel-Lucent and non-Telco device has a generic NE profile; see chapter 13 for more information.

1 Using a CLI, ensure that each device you want to discover and manage using SNMPv3 has a unique engine ID. See Procedure 14-1 for more information.

2 If required, perform the following steps to configure SSH2 security.

i Enable SSH2 on the device. See Procedure 14-2 for more information.

ii Configure and start an SSH server on the device. See the appropriate device documentation for SSH configuration information.

Note — A 7705 SAR may become temporarily unreachable after you enable SSH and start the SSH server on the device.

iii If the device supports SSH2 host key persistence, use Telnet to enable this function on the device. See Procedure 14-3 for more information.

3 Create a mediation policy. If you want to use SSH2 for mediation, ensure that you enable SSH2 for CLI sessions and secure file transfers. See Procedure 14-4 for more information.

Note — If you specify the use of SNMPv3 in the policy, you must enable SSH2 in the policy.

4 Discover the devices.

i Create one or more discovery rules, as required. See Procedures 14-5 and 14-6 for more information.

Note — If you want to use SSH2, specify the created SSH2 mediation policy for read and write access in the discovery rule.

ii Verify the discovery, management, and synchronization statuses of each device specified in the discovery rules.

5 As required, create event notification policies. See Procedure 14-7 for more information.

6 As required, assign event notification policies to NEs. See Procedure 14-8 for more information.

7 As required, manage device discovery by performing one or more of the following using the procedures in this chapter.

a Edit discovery rules and rule elements. See Procedure 14-9 for more information.

b Enable or disable discovery rules. See Procedure 14-10 for more information.

c Delete discovery rules. See Procedure 14-11 for more information.

d Rescan the network using a discovery rule. See Procedure 14-12 for more information.

e Manage, unmanage, or delete managed devices. See Procedures 14-13, 14-14, and 14-15 for more information.

f Synchronize NEs with the 5620 SAM database. See Procedure 14-16 for more information.

g Monitor the acceptance and rejection of SSH2 host keys using the 5620 SAM SSH2 Known Host Key Manager. See Procedure 14-17 and 14-18 for more information.

h Switch from non-secure to secure mediation for one or more devices. See Procedures 14-19 and 14-20 for more information.

i List and save SNMP MIB information. See Procedure 14-21 for more information.

14.8 Device discovery procedures

Use the following procedures to configure device discovery and mediation.

Procedure 14-1 To configure SNMPv3 on a device

Perform this procedure to enable SNMPv3 on a device. SNMPv3 provides user-based security. The access granted is restricted to the scope of the configured users and groups.

If you are configuring an NE for LI, you must create a second access group. See step 2 in Procedure 34-3 for more information about creating an LI user and access group.

1 Open a CLI session on the device.

2 Enter the following commands in the order shown to create a read-write-notify group for general SNMP mediation on the managed device:

configure system security snmp ↵

access group "*snmpv3_groupname*" security-model usm security-level privacy read "iso" write "iso" notify "iso" ↵

where
snmpv3_groupname is the name that is being assigned to the SNMP group

3 If mediation of VPRN objects is required, enter the following command to create a read-write-notify group for this purpose on the managed device:

access group "*snmpv3_groupname*" security-model usm security-level privacy context vprn prefix read "vprn-view" write "vprn-view" notify "iso" ↵

where
snmpv3_groupname is the name that is being assigned to the SNMP group

4 Enter the following command to exit SNMP group configuration.

exit ↵

5 Enter the following command to obtain the SNMP engine ID of the device.

show system info ↵

The SNMP engine ID is displayed as SNMP Engine ID.

6 Generate an MD5 or SHA authentication key, and DES privacy keys, using the password2key utility on a 5620 SAM client or server station.

- MD5 and SHA authentication keys are used to create an encrypted authentication password for users.
- DES privacy keys are used to encrypt the entire SNMP packet, for additional security.

Note — The length of a generated key is determined by the authentication method. MD5 keys are 32-character strings. SHA keys are 40-character strings.

i Log in to the 5620 SAM client or server station.

Note 1 — If you are using the password2key utility on a Solaris 5620 SAM server station, you must log in as the samadmin user.

Note 2 — If you are using the password2key utility on a 5620 SAM client station, you must log in as a local administrator, or as the user that installed the client.

ii Open a console window.

iii Navigate to the *install_directory*/nms/bin directory

where *install_directory* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on Solaris, or C:\5620sam\client on Windows

iv Enter the following to create an MD5 or SHA authentication key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the authentication key, either MD5 or SHA
password is the ASCII password string used to generate the authentication key for the SNMPv3 user, for example, yoga
engine_ID is the SNMP engine ID obtained in step 5

The SHA authentication key generated from this example is 60210e3d2bfa7e02682262df9c5de400b9c3322b.

v Enter the following to create an MD5 or SHA DES privacy key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the DES privacy key, either MD5 or SHA
password is the ASCII password string used to generate the DES privacy key, for example, happy
engine_ID is the SNMP engine ID obtained in step 5

The DES privacy key generated from this example is 4088f4ef966b8d1ebe54b8d841a5f76806c374ec.

vi If your security model requires unique keys for each managed device, repeat steps 6iv and 6v for each set of keys to be generated.

vii Store the generated keys.

7 Using the keys generated in step 6, create an SNMPv3 user on the managed device.

i Enter the following sequence of commands at the prompt:

configure system security user *snmpv3_username* ↵

access snmp ↵

snmp ↵

authentication *method authentication_key* privacy des-key *DES_privacy_key* ↵

group *snmpv3_groupname* ↵

exit all ↵

where
snmpv3_username is the name being assigned to the SNMPv3 user
snmpv3_groupname is the name of the new SNMP user group
method is sha or md5, depending on the authentication method used
authentication_key is the SHA or MD5 authentication key generated in step 6
DES_privacy_key is the DES privacy key generated in step 6

Note — A DES privacy key is 32 characters long. If SHA encryption, which produces a 40-character key, is used to generate the DES privacy key in step 6, you must provide only the first 32 characters of the key, as shown in the following example that uses the key values from step 6:

authentication sha 60210e3d2bfa7e02682262df9c5de400b9c3322b privacy des 4088f4ef966b8d1ebe54b8d841a5f768 ↵

ii Enter the following command at the prompt to save the configuration changes.

admin save ↵

The device is now ready to be managed using SNMPv3. To enable device management by the 5620 SAM, you must do the following:

- Create an SNMPv3 user using the 5620 SAM NE user configuration manager. See chapter 21 for information about creating and configuring NE users. You must specify the following for each user:
  - Give the user SNMP access.
  - Enter the same User Name as the user name created earlier in this procedure.
  - On the SNMPv3 tab, select SHA as the authentication protocol and DES as the privacy protocol.
  - Type the appropriate ASCII password used to generate the MD5 or SHA authentication key, and DES privacy key, in step 6; for example, yoga and happy.
- Create a new SNMPv3 mediation security policy, as described in Procedure 14-4. Specify the following:
  - the SNMPv3 USM security model
  - the SNMP user name created earlier in this procedure
- Create one or more discovery rules that use the new SNMPv3 mediation policy.

8 Close the CLI session.

Procedure 14-2 To verify that SSH2 is enabled on a device

Perform this procedure to verify that SSH2 is enabled on a device, and to enable SSH2 on the device, if required. See section 14.4 for a list of devices that support SSH2.

Note — If the device is a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA, you cannot use this procedure to enable SSH2. You must see the device documentation for information about enabling SSH2.

1 Open a CLI session on the device.

2 Run the following CLI command to see whether SSH2 is enabled:

```
show system security ssh ↵
```

3 If required, enter the following command at the prompt to enable SSH2:

```
configure system security ssh version 2 ↵
```

4 Close the CLI session.

Procedure 14-3 To enable host key persistence on the SSH2 server of a device

Perform this procedure to enable the persistence of the server host key on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, 7750 SR, 7705 SAR, or 7710 SR. Host key persistence is always enabled on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA. For other devices, see the user documentation for information about configuring SSH2 host key persistence.

1 Open a CLI session on the device.

2 Enter the following at the prompt to disable the SSH server:

configure system security ssh server-shutdown ↵

3 Enter the following at the prompt to enable host key persistence:

configure system security ssh preserve-key ↵

4 Enter the following at the prompt to enable the SSH server:

configure system security ssh no server-shutdown ↵

5 Enter the following at the prompt to verify that the preserve-key function is enabled on the server:

show system security ssh ↵

6 Close the CLI session.

Procedure 14-4 To configure NE mediation

Perform this procedure to configure the 5620 SAM to poll network elements at regular rates and intervals. To configure LI mediation, see Procedure 34-5.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Polling Synchronization Time
- Polling Admin State
- Discovery Rule Scan Interval

Note — Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities when setting these parameters.

3 Configure MIB polling intervals for different managed devices, as required.

i Click on the MIB Entry Policies tab button.

A list of MIBs appears, organized by the product name of the device that supports the MIB.

ii Configure the search filter and click on the Search button. The Mediation (Edit) form displays the MIB entry policies that match the search criteria.

iii Select one or more MIBs from the list.

iv Click on the Properties button.

The MIB Entry Policy (Edit) form opens.

v Configure the parameters:

- Polling Interval
- Administrative State
- Number of Varbind per PDU

Caution — Changing the Number of Varbind per PDU parameter value may affect the time required for subsequent NE resynchronizations and degrade 5620 SAM server performance. Do not configure the parameter without contacting Alcatel-Lucent technical support.

vi Click on the OK button.

vii Confirm the action.

The MIB Entry Policy (Edit) form closes and the Mediation (Edit) form reappears.

viii Click on the Apply button to save the changes, if required.

4 Use the Ping tab to define how the management IP addresses of devices are checked using a ping. Each managed device may provide one or more of the following three IP addresses, each of which can be scheduled to be pinged, as configured during discovery rule creation:

- the system IP address, called an in-band management interface
- the management IP address on the management port, called an out-of-band management interface
- the IP address of the standby Control card, also called a CPM

Note — When the device does not have one or two of the IP addresses, for example, there is no CPM IP address, ensure that you create a ping policy that does not have its schedule enabled. This allows the assignment of an inactive ping policy during discovery configuration. See Procedure 14-6 for more information.

i Click on the Ping tab button.

ii Click on the Create button to create a new ping policy, or click on the Properties button to change an existing ping policy.

The ManagementPingPolicy (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Ping Command Timeout (seconds)
- Schedule Enabled
  You must enable scheduling for the default ping policy to be performed. When scheduling is not enabled, and a managed device is not reachable, management connection alarms may not be raised.
- Ping Interval (minutes)
- Ping Interval (seconds)

The destination interface of the ping is determined during the creation of discovery rules for devices. You can also perform an unscheduled ping from the Managed State tab of the Discovery Manager configuration form. See Procedure 14-6 for more information.

iv Click on the Apply button to save the changes.

You can view management connection alarms from the network element properties form of the managed device that was pinged. For example, from the Discovery Manager form, click on the Resync Status tab button. Choose a device from the list and click on the Properties button. From the network element properties form, click on the Faults tab button to view the alarms.

5 Create or modify a statistics MIB policy to determine how often the 5620 SAM polls the managed device MIBs for statistics. See the *5620 SAM Statistics Management Guide* for more information.

6 Click on the Mediation Security tab button.

i Click on the Create button to create a new SNMP mediation security policy, or select an existing policy and click on the Properties button to modify the policy. The MediationPolicy form opens.

Note 1 — Each 7250 SAS or Telco device requires a separate mediation policy unless the user names and passwords, which are often the SNMP community strings, match exactly.

Note 2 — To configure SNMPv3 security, you must preconfigure the 5620 SAM server and the managed devices. See Procedure 14-1 for more information.

ii Configure the general mediation parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Security Model
- Timeout (milliseconds)
- Retry
- Community String

Note — The Community String value must match the community string value on the managed device.

iii Configure the parameters in the CLI and File Transfer panels:

- Communication Protocol
- User Name
- User Password

  You must also enter the User Password parameter value in the Confirm Password parameter field.
- File Transfer Type

Note 1 — If you choose Secure as the File Transfer Type parameter value, you must set the Communication Protocol parameter to SSH2.

Note 2 — To configure SSH2 you must enable SSH2 and host key persistence on the SSH server of the device. See section 14.4 for more information about configuring SSH2.

Note 3 — If you choose SSH2 as the Communication Protocol, the User Name and User Password parameters must be the user name and password for the SSH server.

Note 4 — You must also enter the User Password value in the Confirm Password field.

7 If you choose SSH2 as the Communication Protocol value in step 6 iii, configure the SSH2 Server Port parameter.

8 Perform one of the following.

a If you choose FTP as the File Transfer Type value in step 6 iii, configure the parameters in the FTP panel:

- User Name
- User Password
  You must also enter the User Password parameter value in the Confirm Password parameter field.
- Read Timeout (sec)
- Read Timeout (sec)

b If you choose Secure as the File Transfer Type value in step 6 iii, configure the parameters in the Secure FTP panel:

- Read Timeout (sec)
- Read Timeout (sec)

See chapter 13 for information about enabling FTP access for a device user account.

9 If you set the Security Model parameter to SNMPv3 (USM), assign a user profile that is configured with the SNMPv3 authentication and privacy parameters, as described in Procedure 14-1.

i Click on the Select button to view a list of configured users. The Select Site User For SNMP Access form opens.

ii Select a user from the list and click on the OK button. The user name is displayed on the Mediation Security form.

iii Click on the Properties button to open the configuration form for the user and view or modify the SNMPv3 security settings, if required.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The Mediation Policy form closes and the Mediation (Edit) form reappears.

12 Close the Mediation (Edit) form.

Procedure 14-5 To configure a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Click on the Create button to create a new discovery rule. The Create Discovery Rule - Specify General Attributes form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Administrative State

  When you set the administrative state to Up, the network is scanned according to the discovery rule when the discovery rule is saved. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the Mediation (Edit) form. When you set the administrative state to Down, the network is not scanned as specified by these conditions.
- OLC State
- Management Protocol
- Default External EMS

4 Click on the select button beside the Group Name parameter. The Select Discovery Group - TopologyDiscoveryRule window opens with a list of Topology Groups.

5 Choose a Topology Group from the list.

6 Click on the OK button. The Create Discovery Rule form refreshes with the Topology Group information displayed.

Note — If the selected Topology Group reaches the maximum element limit, any additional discovered NEs are automatically added to the Discovered Group.

7 Click the Next button. The Create Discovery Rule - Add Rule Elements form opens.

8 Click on the Create button to add a new rule element. The Topology Discovery Rule Element (Create) form opens.

9 Configure the parameters:

- IP Address
- Mask Bits
- Usage

Note — Ensure that you track the IP addresses used to discover devices. When the IP address used to discover the device is the system IP address (also known as the system ID) or the L3 management interface address, management is in band. When the IP address used to discover the device is the management IP address of the device management port, management is out of band.

10 Click on the OK button. The Topology Discovery Rule Element (Create) form closes and the Create Discovery Rule - Add Rule Elements form reappears.

The discovery rule is saved.

11 Confirm the action.

12 Add more rule elements, as required, by performing steps 8 to 10.

13 Click on the next button. The Add Auto Discovery Rule Elements ACL form opens.

14 Click on the Create button. The Auto Discovery Rule Element ACL (Create) form opens.

15 Configure the parameters:

- System ID
- Action

16 Click on the OK button. The Auto Discovery Rule Element ACL (Create) form closes and the Add Auto Discovery Rule Elements ACL form reappears.

17 Add more automatic discovery rule elements, as required, by performing steps 14 to 16.

18 Click on the Next button. The Create Discovery Rule - Configure Mediation Security form opens.

19 Specify the mediation policies for read access, write access, and SNMP trap access. Mediation policies are created or modified using the Mediation form, as described in Procedure 14-4.

Click on the Select button if you want to specify mediation security policies specific to the discovery rule. The Configure Mediation Security form opens.

You can:

- Select an existing mediation security policy from the list and click on the OK button.
- Select an existing mediation security policy and click on the Properties button. The MediationPolicy (Edit) form opens.
- Configure the parameters, as described in step 6 in Procedure 14-4 and click on the OK button to save the changes.

If you do not specify a policy, the default policy is applied.

20 Click on the Next button. The Create Discovery Rule - Configure Management Ping Policy form opens.

21 Specify the management ping policies for each of the following management IP addresses, if required:

- the management IP address on the management port, called an out-of-band management interface
- the system IP address, called an in-band management interface
- the IP address of the standby Control card, also called a CPM

Note — Management ping policies are created using the Mediation configuration form. These are the policies applied during discovery rule creation. You must apply a ping policy even to interfaces that do not exist.

For example, if there is no standby CPM or out-of-band management IP address, specify a ping policy that has the Schedule Enabled parameter set to disabled for the nonexistent management and standby CPM interfaces. In this example, a ping policy with the Schedule Enabled parameter enabled is required for the in-band interface that does exist. See Procedure 14-4 for more information about creating ping policies.

22 Click on the Select button for each ping policy ID parameter. The Configure Management Ping Policy list form opens.

23 Choose a ping policy from the list. When there is no interface, choose a ping policy that has its Schedule Enabled parameter set to disabled.

24 Click on the OK button. The ping policy ID appears in the Policy ID parameter.

You can view management connection alarms from the network element properties form of the managed device that was pinged. For example, from the Discovery Manager form, click on the Resync Status tab button. Choose a device from the list and click on the Properties button. From the network element properties form, click on the Faults tab button to view the alarms.

25 Click on the Next button. The Create Discovery Rule - Configure MIB Statistics Policy form opens with the default MIB statistics policy displayed.

26 Click on the Select button to choose a different MIB statistics policy, if required. The Configure MIB Statistics Policy form opens. Select a MIB statistics policy in the list and click on the OK button.

27 Click on the Next button. The Create Discovery Rule - Add Discovered Routers to Span(s) form opens.

28 Click on the Add button to specify a span of control for the new network element contained in the discovery rule. If you do not specify a span, the default span is applied.

Note — New routers added to a span from a discovery rule are added explicitly to the span.

When a discovered NE group is part of a user-defined span, new routers that are discovered from the discovery rule are automatically added to the span.

29 Click on the Next button. The Create Discovery Rule - Configure Backup Policy form opens.

30 Click on the Select button to choose a different backup policy, if required. The Select Backup Policy - Topology Discovery Rule form opens. Select a backup policy in the list and click on the OK button.

31 Click on the Next button. The Create Discovery Rule - Add EM Systems form opens.

32 Click on the Add... button. The EM System (Create) form opens with the General tab displayed.

33 Configure the parameters:

- Element Manager System Name
- Description
- Administrative State

34 Click on the Element Managers tab button.

35 Click on the Add... button. The Element Manager (Create) form opens.

36 Configure the parameters:

- Host Name
- Server Type
- Server IP Address
- Server Port Number
- User Name
- Password

37 Click on the OK button. The Element Manager (Create) form closes and the EM System (Create) form reappears.

38 Click on the OK button. The EM System (Create) form closes and the Create Discovery Rule - Add EM Systems form reappears.

39 Click on the Finish button. The Create Discovery Rule form closes and a dialog box appears.

Note 1 — If the EM System being discovered is an OMC-RAN, only space and underscore are supported characters for node names. Any other special characters will be replaced by an underscore.

Note 2 — After discovering an EM System, the system should be opened and its administrative state set to Up in order to enable the connection to the 5620 SAM. A maximum of four EM Systems may have their administrative state set to Up at any time within the 5620 SAM.

Note 3 — A manual resynch must be performed in order for alarms from an EM System to be displayed in the 5620 SAM client or Supervision web portal.

40 Click on the OK button to close the dialog box. The Discovery Manager form reappears.

41 Close the Discovery Manager form.

Procedure 14-6 To discover devices

Perform this procedure to complete the following tasks:

- Create discovery rules
- Ping the managed devices to test connectivity
- Locate managed devices on a topology map
- Discover devices by scanning the network according to discovery rules
- Set discovered devices in a managed state
- Resynchronize NEs and the 5620 SAM database
- Check the discovery, management, and synchronization status of a device

Note 1 — SNMP parameters must be correctly specified using CLI on the managed devices. Contact your Alcatel-Lucent support representative or see chapter 13 for more information about using CLI to commission devices before managing them.

Note 2 — Ensure that in-band and out-of-band management are correctly configured to discover devices, as described in chapter 13.

1 Configure a discovery rule as described in Procedure 14-5.

2 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

3 Click on the Apply button to discover devices by scanning the network as specified by a discovery rule.

New or modified discovery rules are saved. The 5620 SAM discovers devices by scanning the network as specified by the discovery rules. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the device elements to the 5620 SAM database.

Discovery rules that are disabled or shut down are not applied.

4 Verify that the device is discovered and is managed by the 5620 SAM by clicking on the Managed State tab button on the Discovery Manager form. A list of managed devices opens.

The management state of the device is displayed in the Site State column. Managed is the default state. If the device is unmanaged, select the device from the list and click on the Manage button.

5 From the Managed State tab, you can also perform management IP address pings to ensure connectivity to all managed devices. Do not ping devices without an interface.

6 From the Managed State tab, you can locate the device in a topology map.

i Click on one or multiple managed devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) window appears showing the selected network objects.

> **Note —** Only managed devices located outside the discovery group can be located. If the selected managed devices do not all belong to the same group on the map, then only the managed devices of one of the groups is located. Unmanaged devices cannot be located.

7 Verify that the device configuration has been reconciled with the 5620 SAM database contents, by clicking on the Resync Status tab button. The Resync Status tab displays the operation status of the last full resync to the user. See section 14.2 for more information.

To initiate manual device reconciliation, select one or more devices in the list and click on the Resync button.

If the reconciliation fails:

- View faults that are associated with a device by double-clicking on the device in the Discovery Manager form and clicking on the Faults tab button in the form that opens.
- Check your SNMP security parameters on a device using the CLI.
- Check your 5620 SAM mediation settings by choosing Administration→Mediation from the 5620 SAM main menu.

Devices that have been successfully discovered appear in the 5620 SAM navigation tree.

8 From the Resync Status tab, you can locate the device in a topology map.

i Click on one or multiple resynchronized devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) window appears showing the selected network objects.

> **Note —** Only devices located outside the discovery group can be located. If the selected devices do not all belong to the same group on the map, then only the devices of one of the groups is located.

9 Close the Discovery Manager form.

Procedure 14-7 To configure an event notification policy

Perform this procedure to configure how the 5620 SAM processes specific SNMP traps from specific NE types and releases.

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens.

2 Click on the Event Notification Policies tab button.

3 Perform one of the following.

a Create a policy.

i Click on the Create button. The Event Notification Policy (Create) form opens.

ii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Description
- Network Element Type

After the Network Element Type parameter is configured, the form expands to display the Product and Version panels.

iii Click on the Select button in the Version panel to choose the version of NE to which the policy is to apply. The Select Version - Event Notification Policy form opens with a list of available versions displayed.

iv Select a version and click on the OK button. The Select Version - Event Notification Policy form closes and the version information is displayed on the Event Notification Policy (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Mediation (Edit) form reappears with the new policy in the list.

vii Click on the Apply button. A dialog box appears.

viii Click on the Yes button.

ix Select the new policy in the list and click on the Properties button. The Event Notification Policy (Edit) form opens.

b Modify a policy.

i Click on the Displayed Name column heading to sort the existing policies by device type and version.

ii Drag the Displayed Name column boundary to display the device type and release information.

iii Scroll through the list to locate the policy for the required device type and version using the information in the Displayed Name column.

iv Select the required policy and click on the Properties button. The Event Notification Policy (Edit) form opens.

v Configure the parameters:

- Displayed Name
- Description

4 Click on the Notification Policies tab button. A list of SNMP traps is displayed.

5 Click on a column header, for example, MIB Name or MIB Entry Name, to sort the list alphabetically.

6 Select an SNMP trap entry in the list and click on the Properties button. The MIB Entry Policy - trappolicy (Edit) form opens.

7 Configure the Administrative State parameter.

Note — You cannot configure the Administrative State parameter in a default event notification policy. A default policy is indicated by a check mark beside the Default Policy indicator on the General tab of the Event Notification Policy (Edit) form.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MIB Entry Policy - trappolicy (Edit) form closes.

10 Repeat steps 6 to 9 to configure the processing of an additional SNMP trap by the 5620 SAM.

11 Close the Event Notification Policy (Edit) form.

12 Close the Mediation (Edit) form.

Procedure 14-8 To assign an event notification policy to an NE

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you assign an event notification policy to an NE, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Right-click on an NE icon in the navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Polling tab button.

3 Click on the Clear button in the Assigned Event Notification Policy panel. The Select button in the panel is enabled.

4 Click on the Select button in the Assigned Event Notification Policy panel to choose an event notification policy. The Select Event Notification Policy - Network Element form opens with a list of appropriate event notification policies for the device displayed.

5 Select a policy in the list and click on the OK button. The Select Event Notification Policy - Network Element form closes and the new policy identifier is displayed on the Network Element (Edit) form.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes and the policy is applied.

Procedure 14-9 To edit a discovery rule

Edit discovery rules when new devices are added to the network.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Click on the Properties button.

The appropriate TopologyDiscoveryRule (Edit) form opens.

4 Configure the parameters, as required. For example, to remove a rule element:

i Click on the Rule Elements tab button.

ii Select the rule from the list.

iii Click on the Delete button.

iv Confirm the action.

5 Click on the OK button to close the TopologyDiscoveryRule (Edit) form.

6 Perform steps 3 to 7 in Procedure 14-6.

7 Close the Discovery Manager form.

Procedure 14-10 To enable or disable a discovery rule

When a discovery rule is enabled, the network is scanned according to the discovery rule when the discovery rule is saved or rescanned. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the Mediation form. If your discovery rule is disabled, the network is not scanned as specified by these conditions.

1 Choose Administration→Discovery Manager from the main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Enable or disable the discovery rule.

  a Click on the Turn Up button to enable the discovery rule.

  b Click on the Shut Down button to disable the discovery rule.

Procedure 14-11 To delete a discovery rule

When you delete a discovery rule, only the rule is removed; the devices discovered using the rule are not removed from the 5620 SAM.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule in the list.

3 Click on the Delete button. A dialog box appears.

4 Click on the OK button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Discovery Manager form closes.

Procedure 14-12 To rescan the network according to a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select one or more discovery rules from the list.

3 Click on the Rescan button.

4 Click Yes to confirm the action.

The 5620 SAM scans the network as specified by the discovery rules and discovers devices. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the NE properties to the 5620 SAM database.

5 Perform steps 4 and 7 in Procedure 14-6 to verify that the device has been successfully discovered.

Procedure 14-13 To manage or unmanage a device

Warning — Unmanaging a device results in a loss of management data for the selected device. See section 14.1 for more information.

If you use the 5670 RAM to process 5620 SAM statistics, unmanaging an NE results in the loss of all historical 5670 RAM AA statistics for the device.

Manage/unmanage of HIP devices is not supported. To unmanage or delete a HIP network element, you must set the EMS administrative state to down, then delete the EMS.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Select a device in the list.

4 Click on the Manage or Unmanage button, as required. A Confirm message appears.

5 View the information and click Yes to confirm the action.

The device becomes managed or unmanaged by the 5620 SAM.

Procedure 14-14 To specify which management address the 5620 SAM uses to remanage a device

Perform this procedure to specify which management IP address is saved for a device when the device is set to an unmanaged state. You can configure the 5620 SAM to save the original management IP address or the most recently used management IP address for a device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Choose a device from the list.

4 Click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

5 Configure the Use Original Management IP parameter.

6 Click on the OK button. A dialog box appears.

7 Click Yes to confirm the action.

Procedure 14-15 To delete a device

Warning — Deleting a device results in a loss of management data and completely removes the device from the managed network. See section 14.1 for more information.

If you use the 5670 RAM to process 5620 SAM statistics, deleting an NE results in the loss of all historical 5670 RAM AA statistics for the device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Select a device in the list.

4 If the device is managed, click on the Unmanage button and wait for the state to change to Unmanaged, otherwise, go to step 5.

5 Click on the Delete button. A Confirm message appears.

6 View the information and click Yes to confirm the action.

The device is deleted by the 5620 SAM.

Procedure 14-16 To partially or fully resynchronize NEs with the 5620 SAM database

1 Perform one of the following.

a Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

b Open a physical or service tunnel topology map displaying the required NE(s). Refer to Chapter 5 for more information on using topology maps.

2 Select the required NE(s). Multiple selection is allowed.

3 Choose a resynchonization option.

a Right-click on one of the selected devices you want to resynchronize with the 5620 SAM database and choose Resync→Resync All MIBs from the contextual menu.

Note — Choosing Resync All MIBs will fully resynchronize all MIBs for the devices, ignoring timestamps.

b Perform a partial resynchronization.

i Right-click on one of the selected devices you want to resynchronize with the 5620 SAM database and choose Resync→Customized Resync from the contextual menu. The Resync Site(s) form opens.

ii Select Choose MIB Entries.

iii Click on the Next button.

iv Select one or more MIB entries from the list.

v Click on the Next button.

vi Configure the Ignore Timestamps parameter.

vii Click on the Finish button and close the Resynce Site(s) form.

4 Choose Administration→Discovery Manager from the 5620 SAM main menu.

5 Perform step 7 in Procedure 14-6 to verify that a particular device's properties have been added to the 5620 SAM database.

6 Close the Discovery Manager form.

Procedure 14-17 To view the active and mismatched host keys

1 Open the SSH2 known host key manager by performing one of the following.

a Choose Administration→Security→SSH2 Known Host Key from the 5620 SAM main menu.

b Perform the following steps.

i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

ii Click on the Managed State tab button. A list of managed devices appears.

iii Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

iv Click on the Mediation Security tab button.

v Click on the SSH2 Known Host Key button. The SSH2 Known Host Key Manager form opens.

2 Configure the filter criteria. A list of active and mismatched host keys appears.

3 Click on the Close button to close the SSH2 Known Host Key Manager form and the open parent forms, as required.

Procedure 14-18 To manually accept a mismatched host key

Perform this procedure to manually accept a host key that has been rejected by the 5620 SAM client so that a connection to the SSH server can be established. Before you accept a mismatched host key, verify the validity of the connection to the SSH server.

1 Open the SSH2 Known Host Key Manager by performing one of the following.

a Choose Administration→Security→SSH2 Known Host Key Manager from the 5620 SAM main menu.

b Perform the following steps.

i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

ii Click on the Managed State tab button. A list of managed devices appears.

iii Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

iv Click on the Mediation Security tab button.

v Click on the SSH2 Known Host Key button.

The SSH2 Known Host Key Manager filter form opens.

2 Choose Mismatch SSH2 Host Key as a match criterion using the drop-down list in the SSH2 Server Status column header.

3 Click on the Search button. A list of mismatched host keys is displayed.

4 Select the required host key entry.

5 Verify with the device administrator that the key fingerprint is the host key of the required device.

6 Click on the Delete button to delete the mismatched host key. The mismatched host key is deleted and a connection to the SSH server can be established.

Note — You can only remove the mismatched host key entry using the SSH2 Known Host Key Manager form. Deleting a Host Key Mismatch alarm from the dynamic alarm list does not remove the host key from the SSH2 Host Key Manager and 5620 SAM database.

7 Close the SSH2 Known Host Key Manager form.

8 Close the Node Discovery Control (Edit) form, if it is open.

9 Close the Discovery Manager (Edit) form, if it is open.

Procedure 14-19 To change from SNMPv2c management of a device to SNMPv3 management

1 Unmanage and delete the device.

- i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.
- ii On the Discovery Manager (Edit) form, select the device from the list that you want to manage using SNMPv3 and then click on the Unmanage button.
- iii When the device shows a Site State of Not Managed, click on the Delete button.
- iv Click OK on the Discovery Manager (Edit) form.

2 Perform Procedure 14-1 to create SNMPv3 groups and users on the device, and to create a discovery rule with an SNMPv3 mediation security policy.

Note — You can modify the existing discovery rule with an SNMPv3 mediation security policy. However, you must create a new discovery rule for the deleted device if not all devices discovered by the same rule are changed to SNMPv3 management.

3 Rediscover the device.

- i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.
- ii Click on the Discovery Rules tab button.

- **iii** Select the discovery rule that was created in step 2 to discover the deleted device.
- **iv** Click on the Rescan button.
- **v** Click OK on the Discovery Manager (Edit) form.

Procedure 14-20 To switch from non-secure to secure mediation

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the Mediation Security tab button. You can create a mediation policy as described in Procedure 14-4, or modify the default mediation policy to use SSH2. Perform one of the following.

- **a** Click on the Create button to create a new mediation policy. The Mediation Policy (Create) form opens with the General tab displayed.
- **b** Choose the default policy from the list, and click on Edit. The Mediation Policy (Edit) form opens with the General tab displayed.

3 Configure the following parameters using the prescribed values:

- SSH2 as the Communication Protocol
- The SSH2 server user name and password as the User Name and User Password
- Secure as the File Transfer Type

Note — When the File Transfer Type is set to Secure, the Communication Protocol, User Name, and User Password parameters must be configured with the SSH2 information.

- The port that the NE uses for SSH2 communication as the SSH2 Server Port

4 Configure the remaining parameters on the form.

5 Click on the OK button. A dialog box appears.

6 Click on the OK button. The Mediation Policy form closes.

7 Click on the OK button. The Mediation (Edit) form closes.

8 Perform steps 1 to 3 of Procedure 14-6 to create a new discovery rule that uses the new SSH2 mediation policy as the read-access mediation policy and the write-access mediation policy.

9 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

10 Click on the Managed State tab button. A list of managed devices appears.

11 Choose the device from the list that you want to use SSH2 for CLI sessions and secure file transfers.

12 Click on the Properties button.

13 Click on the Mediation Security tab button.

14 Choose the newly created SSH2 mediation policy as the read access mediation policy.

> **Note —** You can also change the mediation policy for a discovery rule by performing step 14 and choosing a discovery rule from the Discovery Rules tab.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Discovery Manager (Edit) form closes.

Procedure 14-21 To list and save SNMP MIB information

Perform this procedure to list and save SNMP MIB information, which may be of use for purposes such as the following:

- to maintain a record of the SNMP MIBs that the 5620 SAM supports
- to compare SNMP MIB support between 5620 SAM releases
- to identify the polling interval for a MIB entry

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the MIB Entry Policies tab button.

3 Configure the search filter and click on the OK button. The Mediation (Edit) form displays the MIB entry policies that match the search criteria.

4 To view the polling interval for a MIB entry, perform the following steps.

i select the MIB entry and click on the Properties button. The MIB Entry Policy (Edit) form opens with the General tab displayed.

ii View the polling interval setting in the Configuration panel.

iii Close the MIB Entry Policy (Edit) form.

5 If required, sort the list according to the contents of a column by clicking on the column header.

6 If required, perform the following steps to save the listed information to a file.

- **i** Right-click on a column header and choose Save to File. the Save As form opens.
- **ii** Use the form to specify the file that is to contain the saved information.
- **iii** Click on the Save button. The information is saved to the specified file.

7 Close the Mediation (Edit) form.

15 — Device CLI sessions

15.1 Device CLI sessions overview

You can perform most NE management functions using the 5620 SAM client GUI. Functions such as the following, however, require CLI access to a managed NE:

- validating GUI configuration actions
- configuring items that the GUI cannot, such as LI user access
- troubleshooting using device debug files

The 5620 SAM client GUI provides CLI access to the managed NEs from the main menu and from NE contextual menus in topology maps and navigation trees.

Note 1 — When you use a CLI to change security parameters on anNE, the changes may not be synchronized with the 5620 SAM and subsequently not displayed in the GUI. For security reasons, the 5620 SAM cannot retrieve parameters such as passwords from an NE. To ensure that the security parameters are synchronized, you must use the client GUI to change the values.

Note 2 — A CLI script that is configured for an OmniSwitch NE can fail if it contains one or more of the following characters:

- ~
- !
- @
- $
- %
- &

Scope of command roles and user permissions on the cli package control CLI command access on an NE. The user permissions are set when security is configured on the NE locally or by using 5620 SAM configuration forms. See chapter 21 for more information about setting NE access privileges.

vi editor support

On the 7750 SR, 7450 ESS, and 7710 SR, Release 8.0 or later, you can use the vi editor to modify local files. For example, after you use the 5620 SAM script manager to create a CLI script, you can use a 5620 SAM CLI session to monitor the script execution on an NE, then use vi to modify the script. The vi editor is available in 5620 SAM Telnet and SSH sessions. It supports the standard vi navigation keys as well as the cursor keys, sometimes called the arrow keys. See the appropriate device documentation for information about the supported vi commands and functions for a specific device.

See the appropriate device documentation for information about the device CLI command structure and usage. See the *5620 SAM Scripts and Templates Developer Guide* for more information about using the 5620 SAM script manager to create CLI scripts.

15.2 Workflow to use a 5620 SAM CLI

The following workflow describes the sequence of high-level tasks required to open and use a device CLI from the 5620 SAM client GUI. The following must be true before you can use the 5620 SAM to open a device CLI using the GUI.

- The 5620 SAM user account has console access privileges on the managed devices; see chapter 9 for more information.
- The Telnet server on the managed devices is started.
- If required, SSH2 is properly configured on the managed devices; see chapter 14 for more information.

1 Configure the 5620 SAM CLI preferences. See Procedure 15-1 for more information.

2 Open a CLI session and log in to a managed device. See Procedure 15-2 for more information.

3 Configure the device, view device information, and modify files, as required.

4 Close the CLI session. See Procedure 15-1 for more information.

15.3 CLI procedures

The following procedures describe how to open CLI sessions using the 5620 SAM and configure the CLI console preferences.

Procedure 15-1 To configure the 5620 SAM CLI console preferences

Perform this procedure to customize the 5620 SAM CLI window settings. You can specify the following:

- the console text style and appearance
- the size of the scrolling buffer
- whether to save the session output to a file

1 Open a CLI session, as described in Procedure 15-2.

2 Right-click in the CLI window and choose Configure from the contextual menu. The Terminal Configuration form opens.

3 Configure the parameters:

- Minimum number of scrolling lines
- Font Name
- Font Size
- Bold
- Italic
- Foreground color
- Background color
- Send Console To a File
- Append to file
- Log File Location

Note — When the Send Console To a File parameter is enabled and the Append to file parameter is disabled, the log file is overwritten each time a new CLI session starts.

4 Click on the OK button. The Terminal Configuration form closes. The current and subsequent CLI sessions use the new settings.

Procedure 15-2 To open and close a 5620 SAM device CLI session

Perform this procedure to open a Telnet or SSH session on a managed device using the 5620 SAM client GUI.

1 Perform one of the following.

a Use the 5620 SAM navigation tree; perform the following steps.

i Choose Equipment from the view selector.

ii Right-click on a device icon.

iii Choose NE Sessions→*option* from the contextual menu

where *option* is Telnet Session or SSH Session

The Telnet Session or SSH Session window opens.

Note 1 — The managed device must be configured for Telnet access. See the appropriate device documentation for information about configuring Telnet access to the device.

Note 2 — SSH2 is used in SSH sessions by default on the 7450 ESS, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7750 SR, 7250 SAS, and generic NEs. Ensure that SSH2 is properly configured on such a device and that an SSH2 mediation policy is specified in the device discovery rule. See chapter 14 for more information about configuring SSH2 security.

b Use the 5620 SAM main menu; perform the following steps.

i Choose one of the following main menu options:

- Tools→NE Sessions→Telnet Session
- Tools→NE Sessions→SSH Session

The Telnet Session or SSH Session window opens.

ii Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of the NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for the NE.

The Connect button is enabled.

iii Click on the Connect button.

c Use the Manage Equipment form; perform the following steps.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Configure the filter criteria and click on the Search button.

iii Select an NE in the list.

iv Click on the NE Sessions button and choose Telnet Session or SSH Session. The Telnet Session or SSH Session window opens.

d Use a service topology map; perform the following steps.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

The appropriate management list form opens.

ii Configure the filter criteria and click on the Search button.

iii Select a service in the list.

iv Click on the Topology View button. A dialog box appears.

v Click on the Yes button. A service topology map opens.

vi Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

e Use the Physical Topology map; perform the following steps.

i If the Physical Topology map is not open, choose Application→Physical Topology from the 5620 SAM main menu. The Physical Topology map opens.

ii Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

2 Enter the login credentials. You can use the CLI as specified by your user account permissions.

3 Perform NE management tasks, as required.

4 Click on the Disconnect button to close the CLI session.

Note — When you disconnect from a CLI session, the session window remains open to facilitate the opening of a subsequent CLI session.

5 Perform one of the following.

a Open a new CLI session; perform the following steps.

i Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of an NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for an NE.

The Connect button is enabled.

ii Click on the Connect button.

b Close the Telnet Session or SSH Session window.

16 — Working with network objects

16.1 Working with network objects overview

The 5620 SAM is used to create, configure, and manage a device with the various children objects required to be part of a network. Equipment such as the routers, which are at the top of the hierarchy, have properties that are configured using the CLI and discovered when the 5620 SAM discovery process is run. After the device is discovered, it is displayed as an object in the navigation tree. See chapter 4 for more information about the navigation tree.

Objects in the 5620 SAM are considered to have parent/child relationships that are contained within a hierarchy. For example, a card in a card slot is the parent object of a daughter card. The behavior of each object is defined using parameters that are specific to the function required. Those parameters can be managed to suit the needs of the service required. Objects are created and managed using the properties forms found in the contextual menus of the equipment view.

The network is the top object in the navigation tree. The network icon in the navigation tree is the parent object of all managed devices. When you expand the network icon, all managed devices are shown as children of the network parent.

The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon. The following children objects of the router are created automatically in the navigation tree after the device is discovered.

- CCAG
- ISA-Tunnel Group
- ISA-AA Group
- ISA-LNS Group
- ISA-NAT Group
- ISA-Video Group
- LAG
- IGH
- Shelf
- Card Slot
- Card Slot A for the CPM and switch fabric
- Card Slot B for the redundant CPM and switch fabric
- Fans
- Power Supplies

The following objects must be created using property forms or create forms from the contextual menus of the equipment view or the ring group view.

- topology groups
- individual CCAGs with VSM-CCA members
- individual ISA-Tunnel Groups with ISA IPsec MDA members
- individual ISA-AA Groups with ISA-AA MDA members and ISA-AA partitions
- individual ISA-LNS Groups with ISA broadband applications MDA members
- individual ISA-NAT Groups with ISA broadband applications MDA members
- individual ISA-Video Groups with ISA-Video MDA members
- individual LAGs with subgroups of LAG member ports
- IGH members
- cards
- ring groups

- daughter cards
  Ports are automatically created when the daughter card is created.
- channels

Configuring an object is accomplished in two steps. First the object must exist or be created, second, the object parameters are modified. See Procedure 17-1 to create objects using the navigation tree.

16.2 Working with topology group objects

The topology group icons in the navigation tree represent logical topology groups. Initially, a topology group object is created by choosing Create→Equipment→Group from the 5620 SAM main menu. A Group (Create) form opens. Additional topology groups can be created using the Copy button on the topology group properties form.

The Discovered NEs and the Unmanaged NEs topology groups are created by default. The Discovered NEs topology group contains the discovered devices. The Unmanaged NEs topology group contains unmanaged NEs that have been added to the network. You can create new topology groups and move devices to them using the topology maps.

Note — For existing topologies, the unmanaged NE will not be automatically moved to the Unmanaged NEs topology group in the following situations:

- existing unmanaged NEs
- managed NEs that are unmanaged

Although there is no limit to the number of topology groups, Alcatel-Lucent recommends a maximum of 10 000 topology groups per system for optimal performance. Each topology group can contain a maximum of 500 objects. Network elements and immediate child groups are considered objects in a topology group. A bracketed number is displayed beside the name of each topology group in the navigation tree. This number indicates the current number of objects in the group.

See chapter 5 for information about configuring topology group objects and managing topology groups using maps.

16.3 Working with physical links

The 5620 SAM allows you to create and manage links at the Layer 1 level. The physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the physical topology map and the Manage Equipment list form.

Although there is no limit to the number of physical links you can have in a system, Alcatel-Lucent recommends a maximum of 10 000 physical links for optimal system performance.

Radio links between 9500 MPRs are shown as physical links by the 5620 SAM, with ports as the endpoint type.

See chapter 5 for information about configuring physical links and managing physical links using maps.

16.4 Workflow to manage network objects

The following workflow describes the sequence of high-level tasks required to manage and configure network objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — Network objects can be accessed using the equipment navigation tree. See chapter 4 for more information.

1 As required, create network topology groups. See chapter 5 for more information.

2 As required, configure device objects. See chapter 17 for more information.

3 As required, configure logical group objects. See chapter 18 for more information.

4 As required, configure shelf, card, and daughter card objects. See chapter 19 for more information.

5 As required, configure port and channel objects. See chapter 20 for more information.

6 As required, create physical links. See chapter 5 for more information.

17 — Device object configuration

17.1 Device object configuration overview

The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon.

This chapter contains the procedures to configure device objects using the navigation tree. Device object properties forms, which are used to configure specific parameters for discovered devices, are accessed using objects on the 5620 SAM navigation tree. See chapter 4 for more information about using the navigation tree.

17.2 Working with device objects

The device icons in the navigation tree represent device objects. Most of the configured properties for this object are inherited from the device. The Properties contextual menu option from the navigation tree allows you to configure or modify parameters for the object. These parameters are found on the respective tab buttons of the properties form and include the following:

- General
- Polling
- Protocols
- Load Balancing
- PAE Site
- Groups
- SAS Agent
- Faults

See chapter 13 for in-band and out-of-band management using parameters on the Polling tab. See chapter 12 for more information about the supported device types.

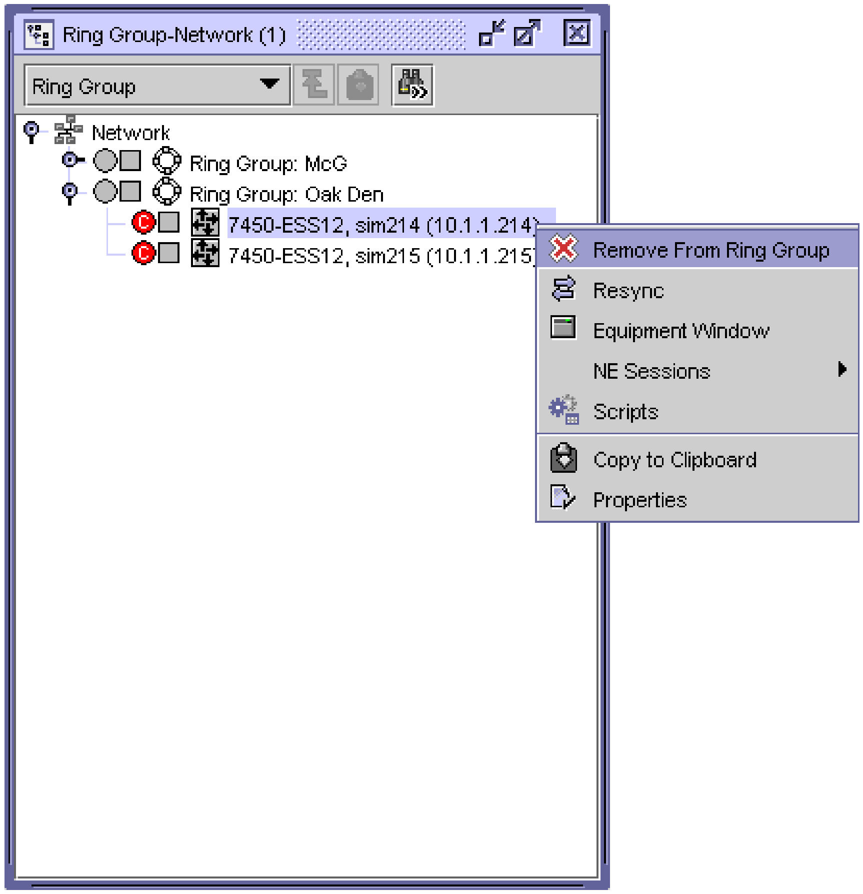
17.3 Working with ring group objects

The 5620 SAM allows you to create and manage ring groups in the ring group view of the navigation tree. Ring groups are used to group devices, such as Telco, 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESAs logically to represent a typical network topology.

Note — The 5620 SAM Release 7.0 R3 or later uses VLAN groups instead of ring groups to group OmniSwitch NEs. When you upgrade to 5620 SAM Release 7.0 R3 or later, a ring group that contains OmniSwitch NEs is automatically converted to a VLAN group. See chapter 70 for more information about VLAN groups.

In the ring group view of the navigation tree, the network icon provides the contextual menu option Create Ring Group to create ring group icons. Using the properties form of a ring group, you can group devices logically in the ring group. Figure 17-1 shows a sample navigation tree ring group view.

Figure 17-1 Sample navigation tree ring group view



17.4 Workflow to manage device objects

The following workflow describes the sequence of high-level tasks required to manage and configure device objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — Device objects can be accessed using the equipment navigation tree. See chapter 4 for more information about using the equipment navigation tree.

1 As required, configure the following general NE capabilities:

- **a** Create an object. See Procedure 17-1 for more information.
- **b** Modify an NE configuration. See Procedure 17-2 for more information.
- **c** Create an operational group. See Procedure 17-3 for more information.

- **d** Enable and configure global Cflowd parameters on an NE, and create Cflowd collectors. See Procedure 17-4 for more information.
- **e** Associate a span of control with an NE. See Procedure 17-5 for more information.
- **f** Configure 802.1x authentication on an NE. See Procedure 17-6 for more information.
- **g** Configure active card alarms on an NE. See Procedure 17-7 for more information.
- **h** Configure a TWAMP server. See Procedure 17-8 for more information.
- **i** Enable LLDP on a router. See Procedure 17-9 for more information.
- **j** Create a chassis-level PBB configuration. See Procedure 17-10 for more information.
- **k** Enable frame-based accounting on a 7210 SAS. See Procedure 17-11 for more information.
- **l** Configure the use of vendor-specific ICMP extensions on a 7705 SAR. See Procedure 17-12 for more information.
- **m** Configure the QoS ingress aggregate rates on a 7705 SAR-M. See Procedure 17-13 for more information.
- **n** Start the 9500 MPR external element manager from the 5620 SAM GUI. See Procedure 17-14 for more information.
- **o** Start and stop a Webview or Secure Webview session on an OmniSwitch. See Procedure 17-15 for more information.
- **p** Configure dying gasp on an OS 6250 (Metro) NE. See Procedure 17-16 for more information.
- **q** Configure port and queue statistics on an OS 6250 port. See Procedure 17-17 for more information.
- **r** Configure Ip statistics on an OmniSwitch routing instance. See Procedure 17-18 for more information.

2 As required, configure ring group objects. See Procedures 17-19 and 17-20 for more information.

3 As required, configure circuit emulation functions as follows:

- **a** Configure a CES module. See Procedure 17-21 for more information.
- **b** Configure a CES port. See Procedure 17-22 for more information.
- **c** Configure an unstructured CES interface. See Procedure 17-23 for more information.
- **d** Configure a structured CES interface. See Procedure 17-24 for more information.
- **e** Modify a CES interface. See Procedure 17-25 for more information.

17.5 General device configuration procedures

Use the following procedures to configure devices using the navigation tree.

Procedure 17-1 To create an object

1 Right-click on an empty object in the navigation tree to open the contextual menu.

2 Choose Properties or, when available, Create <*objectname*>.

The properties form or the create form, as applicable, opens.

3 Configure the parameters as required.

Certain object parameters are available for configuration. Configuring these parameters creates the object, however, after the object is created you may need to edit it using properties forms.

Procedure 17-2 To change device properties

1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

2 Use the properties form to view or modify the device parameters, as required using the following tabs.

- The General tab displays:
  - the Location, Resource Group ID, Latitude (degrees), and Longitude (degrees) parameters
  - the VPLS Mode parameter if the device is a 7250 SAS-ES or 7250 SAS-ESA
  - an Auto-Provision button if the device is a 7705 SAR; see chapter 29 for information about configuring and deploying configuration profiles to a 7705 SAR
  - the Physical Impedance parameter if the device is a 9500 MPR
- The Polling tab displays polling parameters. See chapter 14 for more information about configuring in-band or out-of-band polling policies.
- The Protocols tab displays the routing protocols configured for the device. See chapter 31 for more information about configuring protocols.
- The Inventory tab contains a filterable list where inventory data for the selected NE can be generated.
- The Globals tab contains multiple tabs. Not all tabs apply to every NE type:
  - Load Balancing—displays the L4 Load Balancing parameter
  - Alarm Management—displays the Alarm Management and Maxiumum Cleared Alarms parameters
  - LACP—displays the LACP System Priority parameter
  - LLDP—displays several LLDP parameters. The parameters displayed vary according to the NE type.

    7210 SAS, 7450 ESS, 7710 SR, 7710 SR, and 7750 SR NEs display the Administrative Status, Transmission Interval (Seconds), Transmission Multiplier, Re-Init Delay (Seconds), Notification Interval (Seconds), Maximum Consecutive Transmissions, Fast Transmission Interval (Seconds), and PDUs in Fast Transmission parameters.

    OmniSwitch NEs display the Transmission Interval (Seconds), Transmission Multiplier, Re-Init Delay (Seconds), Notification Interval (Seconds), and Transmission Delay (Seconds) parameters.
  - Ethernet CFM—displays the MEP ID parameter, which is used for automatic MEP ID assignment during automatic MEP creation, the parameters required to enable SLM, and the MC-LAG Standby Inactive and MC-LAG Prop Hold Time parameters. The latter two parameters must be configured for Ethernet CFM redundancy to be operational. See chapter 80 for more information.
  - PAE—displays the Administrative State parameter
  - TWAMP—displays the parameters required to enable TWAMP on a server
- The ATM tab for a 7750 SR displays ATM OAM loopback parameters for interfaces that host IES and VPRN SAPs. See Procedure 38-34 for more information.
- The Scripts tab displays the script instances and versions that are applied to the device. In addition, you can execute scripts and open the script manager using this tab. See the *5620 SAM Scripts and Templates Developer Guide* for more information.
- The Redundancy tab displays two sub-tabs: BGP Multi-homing and MC Peer. The BGP Multi-homing tab allows you to configure NE-level parameters used in

BGP VPLS multi-homing. See Procedure 71-6 for more information. The MC Peer sub-tab allows you to add or remove MC peers. See chapter 41 for more information.

- The Ring Groups tab displays the ring groups associated with the device. See Procedure 17-19 for more information.
- The Rule-Based Groups tab displays the rule-based groups that support rule-based service-tunnel creation.
- The CFLOWD tab displays global NE Cflowd parameters, and allows the configuration of NE-based Cflowd collectors.
- The Frame Based Accounting tab displays the parameters that enable ingress and egress frame-based accounting for the 7210 SAS-E, Release 1.0 R5 or later, the 7210 SAS-M 24F, Release 1.1 R3 or later, and the 7210 SAS-M 24F 2XFP and 7210 SAS-M 24F 2XFP ETR, Release 1.0 R1 or later.
- The Split Horizon Groups tab lists the SHGs that include the device as a member.
- The LI Configuration Status tab which is viewable by an operator with LI privileges, displays the LI operational configuration. See chapter 34 for more information about configuring LI.
- The QoS tab displays the QoS Classification parameter for a 9500 MPR.
- The VLAN Groups tab displays VLAN group information for a 9500 MPR.
- The System Settings tab displays the Admission Control parameter for a 9500 MPR.
- The Physical Links tab displays physical link information. Only radio link information is displayed for the 9500 MPR. See chapter 5 for more information.
- The NE Time configuration tab displays the Network Element Time parameter for a 9500 MPR.
- The Spans tab displays the spans of control. See chapter 9 for more information about configuring a span of control on an NE.
- The Statistics tab displays statistics available for the device. See the *5620 SAM Statistics Management Guide* for more information.
- The Faults tab displays the network-level alarms for the device.

3 Close the device properties form.

Procedure 17-3 To create an operational group

Multiple objects can be bundled into operational groups. Altering the status of the operational group will alter the status of every object contained therein.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an NE in the Equipment view and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Click on the Service tab button.

5 Click on the Operational Group tab button.

6 Click on the Create... button. The Operational Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Group Name
- Hold Down Time
- Hold Up Time

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Operational Group (Create) form closes and the Network Element form reappears with the new operational group in the list.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Network Element form closes.

Procedure 17-4 To enable and configure global Cflowd on an NE

Perform this procedure to enable Cflowd and configure global Cflowd parameters on an NE. You can also configure Cflowd sampling for AA flows. See chapter 77 for information about configuring Cflowd collectors for AA applications groups.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the NE where you want to configure Cflowd and select Properties from the contextual menu. The NE properties form opens.

3 Click on the CFLOWD tab button. The General tab is displayed.

4 Set the CFLOWD State parameter to Enabled. The form displays additional parameters.

5 Configure the remaining parameters:

- Active Time-out (minutes)
- In-Active Time-out (seconds)
- Cache Size
- Sample Rate
- Over Flow (percent)
- Administrative State
- Template Re-transmit (seconds)

6 Click on the Collector tab button.

7 Perform the following steps to add a collector.

i Click on the Create button. The Cflowd Collector Configuration (Create) form opens.

ii Configure the parameters:

- Host Address
- Port Number
- Description
- Version
- Aggregation Type
- Autonomous System
- Template Type

The Aggregation Type parameter is configurable when the Version parameter is set to version-8.

The Autonomous System parameter is configurable when the Version parameter is set to version-5 or version-8.

The Template Type parameter is configurable when the Version parameter is set to version-9.

iii Click on the OK button. The CFLOWD Collector Configuration (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the NE properties form.

8 Repeat step 7 to add another collector, if required.

Note — A global NE Cflowd configuration can contain a maximum of five collectors.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The NE properties form closes.

Procedure 17-5 To add a span of control to an NE

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

3 Click on the Spans tab button.

4 Click on the Add button. The Select Span(s) - Network Element form opens with a list of available spans.

5 Choose one or more spans to apply to the NE.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Select Span(s) - Network Element form closes.

Procedure 17-6 To enable or disable 802.1X

You can view the status of 802.1X authentication on a device in a managed network.

Note — Before you can create an 802.1X policy, 802.1X must be enabled on the device. Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the device and an 802.1X policy must be created and distributed to the device.

1 Enable 802.1X on a managed device:

- i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
- ii Right-click on the managed device where you want to enable or disable 802.1X and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
- iii Click on the Globals tab button. The Load Balancing tab opens.
- iv Click on the PAE tab button.
- v Set the Administrative State parameter to Up.
- vi Click on the OK button. The Network Element (Edit) form closes.
- vii Repeat step 1 for each device for which you want to enable 802.1X.

  To create and distribute 802.1X policies to the devices that use 802.1X, see chapter 54.

  To configure 802.1X on Ethernet access ports, see Procedure 20-1 in chapter 20.

2 To disable 802.1X on a managed device, repeat step 1 but set the Administrative State to Down.

Procedure 17-7 To configure active card alarms on an NE

Use this procedure to configure a 7450 ESS, 7710 SR, or 7750 SR to view NE alarms through the CLI.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Right-click on the NE on which you want to configure active card alarms and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. Click on the Globals tab button. The Load Balancing tab is displayed.
4. Click on the Alarm Management tab button and configure the parameters:
   - Alarm Management
   - Maxiumum Cleared Alarms
5. Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-8 To configure a TWAMP server

You can enable or disable Two-Way Active Measurement Protocol on a server and view session and connection statistics.

Note — You cannot configure a TWAMP server after an NE upgrade until the NE is fully resynchronized.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Right-click on the managed device where you want to configure a TWAMP server and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. Click on the Globals tab button. The Load Balancing tab is displayed.
4. Click on the TWAMP tab button. The General tab is displayed.
5. Configure the Administrative Status parameter.

Note — To make changes to the following TWAMP server parameters, the Administrative Status parameter must be set to disabled.

6 Configure the parameters:

- Inactivity Timeout (Seconds)
- Maximum Connections
- Maximum Sessions

7 Click on the Prefix tab button.

Note — The objects listed in the table control the behavior of the TWAMP connections that match the defined IP prefix.

8 Perform one of the following:

a Click on the Create button to add a new prefix. The Prefix TWAMP Server (Create) form opens, with the General tab displayed.

b Click on the Search button to display a list of existing prefixes. Select the required item from the list and click the Properties button. The Prefix TWAMP Server (Edit) form opens, with the General tab displayed.

9 Configure the parameters:

- Prefix Address
- Prefix Length
- Description
- Maximum # Connections
- Maximum # Sessions

10 Click on the Statistics tab.

11 Select either SrvConnStats (Assurance) or PrefixSrvStats (Assurance), as required, from the Select Object Type drop-down menu.

12 Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.

13 Click on the Statistics Policies button and select Statistics Policy from the menu. The Statistics Policy form opens, with the General tab displayed.

14 Configure the parameters:

- Retention Time (hours)
- Administrative State
- Threshold Reporting State

15 Click on the Thresholds tab.

16 Perform one of the following, depending on your selection in step 11.

a Configure the PrefixSrvStats (Assurance) threshold parameters:

- Srv Pfx Conn Count Periodic Threshold
- Srv Pfx Conns Rejected Periodic Threshold
- Srv Pfx Session Count Periodic Threshold
- Srv Pfx Test Packets Rx Periodic Threshold
- Srv Pfx Test Packets Tx Periodic Threshold
- Srv Pfx Test Sess Abort Periodic Threshold
- Srv Pfx Test Sess Completed Periodic Threshold
- Srv Pfx Test Sess Rejected Periodic Threshold

b Configure the SrvConnStats (Assurance) threshold parameters:

- Conn Idle Time Periodic Threshold (seconds)
- Conn Session Count Periodic Threshold
- Conn Test Packets Rx Periodic Threshold
- Conn Test Packets Tx Periodic Threshold
- Conn Test Sess Completed Periodic Threshold
- Conn Test Sess Rejected Periodic Threshold

17 Click on the OK button. A confirmation dialog is displayed.

18 Click Yes. The Statistics Policy form closes.

19 Click on the OK button. The Prefix TWAMP Server (Create) form closes.

20 To view TWAMP statistics on a server:

i Perform steps 1 to 4 above.

ii Click on the Prefix tab button.

iii Click on the Search button to display a list of existing prefixes. Select the required item from the list and click the Properties button. The Prefix TWAMP Server (Edit) form opens, with the General tab displayed.

iv Select either SrvConnStats (Assurance) or PrefixSrvStats (Assurance), as required, from the Select Object Type drop-down menu.

v Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.

vi Click on the Collect or Collect All button. The system compiles the statistics and displays the available records in the table.

vii Select the required record from the table and click the Properties button. The Statistics Record is displayed.

viii Close the Statistics record form when your are finished.

ix Click on the OK button. The Prefix TWAMP Server (Create) form closes.

21 Close the Network Element (Edit) form.

LLDP

Link Layer Discovery Protocol, or LLDP, is a neighbor-discovery protocol that allows an NE to advertise its identity and capabilities to other NEs attached to the same physical IEEE 801 LAN. LLDP is a global NE function that you can configure from the 5620 SAM equipment navigation tree on NEs that use Ethernet connectivity.

The 5620 SAM supports LLDP configuration on the following devices:

- 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, and 7210 SAS-M 24F 2XFP ETR, Release 3.0 R1 or later
- 7450 ESS
- 7710 SR
- 7750 SR
- OmniSwitch, Release 6.3.1 or later
- OS 6900, Release 7.2.1 or later
- OS 10K, Release 7.1.1 or later

See “LLDP” in section 30.1 for more information about LLDP.

Procedure 17-9 To enable LLDP on a router

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the router icon by choosing Routing→Router.

3 Right-click on the router icon and choose Properties. The Network Element (Edit) form opens.

4 Enable LLDP by performing the following steps.

i Click on the Globals tab button.

ii Configure the parameters:

- Administrative Status
- Transmission Interval (Seconds)
- Transmission Multiplier
- Re-Init Delay (Seconds)
- Maximum Consecutive Transmissions
- Fast Transmission Interval (Seconds)
- PDUs in Fast Transmission
- Notification Interval (Seconds)
- Transmission Delay (Seconds)
- Fast Start Repeat Count

The Administrative Status, Maximum Consecutive Transmissions, Fast Transmission Interval (Seconds), and PDUs in Fast Transmission parameters do not apply to the OmniSwitch.

The Transmission Delay (Seconds) and Fast Start Repeat Count parameter only applies to the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Confirm the action. The Network Element (Edit) form closes.

7 Configure the applicable router ports to fully enable LLDP, as described in step 37 in Procedure 20-1 and step 13 in Procedure 20-34. See step 2 in Procedure 17-2 for information about how to set global node element attributes, including LLDP.

Procedure 17-10 To create a chassis-level PBB configuration

Perform this procedure to provide the PBB MAC name configuration at the NE level.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an NE in the Equipment view and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Click on the Service tab button and configure the parameters:

- PBB Source Backbone MAC Address
- MAC Notification Interval (seconds)
- MAC Notification Count

5 Click on the MAC Name tab button and click on the Create button. The PBB MAC Name (Create) form opens with the General tab displayed. Configure the parameters:

- MAC Name
- MAC Address

6 Click on the OK button.

Procedure 17-11 To enable frame-based accounting for QoS policies

Perform this procedure to enable frame-based accounting for QoS policies on a 7210 SAS-E, Release 1.0 R5 or later, the 7210 SAS-M 24F, Release 1.1 R3 or later, or a 7210 SAS-M 24F 2XFP or 7210 SAS-M 24F 2XFP ETR, Release 1.0 or later.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure frame-based accounting and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Frame Based Accounting tab button.

4 Configure the parameters:

- Egress
- Ingress

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-12 To enable or disable ICMP extensions on the 7705 SAR

Use this procedure to configure the use of vendor-specific ICMP extensions on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR device types.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR where you want to configure ICMP extensions and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the ICMP tab button.

4 Configure the Vendor-Specific ICMP Extensions parameter.

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-13 To configure QoS ingress aggregate rates on the 7705 SAR-M/ME

Perform the following procedure to configure QoS access ingress and network ingress aggregate rates on the 7705 SAR-M/ME.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR-M/ME on which you need to configure QoS ingress aggregate rates and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the QoS tab button.

4 Configure the Aggregate Rate parameter in the Access Ingress panel and in the Network Ingress panel.

5 Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-14 To start the 9500 MPR external element manager from the 5620 SAM GUI

Perform the following procedure to start the 9500 MPR external element manager, NEtO, from the 5620 SAM GUI.

Warning — When you use the 5620 SAM to manage the 9500 MPR, use of the NEtO external element manager must be restricted to configuring only radio modem card parameters. If you use NEtO to configure any other parameters, services can be affected and can seriously impact network management and 5620 SAM performance.

Prerequisite:

- To be able to launch NEtO, you need to define the NEtO path. See Procedure 13-15 for more information on how to define the path.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a discovered 9500 MPR in the Equipment view and choose External Element Manager from the contextual menu. The NEtO main view screen appears.

See the appropriate 9500 MPR *User Guide* for information about configuring and using the NEtO external element manager.

Procedure 17-15 To start and stop a Webview or Secure Webview session on an OmniSwitch

Perform the following procedure to start and stop a Webview or Secure Webview session on an OmniSwitch.

1 To start a Webview or Secure Webview session:

i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

ii Right-click on a discovered OmniSwitch in the Equipment view and choose Launch Webview or Launch Secure Webview from the contextual menu. A web browser starts and the Webview or Secure Webview login screen appears.

Note — An alternative method of launching a Webview or Secure Webview session is to right-click on a discovered OmniSwitch in the Equipment view. Select Equipment Window from the contextual menu. The Equipment Window form opens. Select the Launch Webview or Launch Secure Webview button on the form.

iii Enter your user name and password. After a successful login, the Chassis Management Home Page appears.

2 To stop a Webview or Secure Webview session:

i Click on the Log Out text at the top of the Webview or Secure Webview window. A Confirm Log Out dialog box appears.

ii Click on the Log Out button to end the Webview or Secure Webview session.

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using Webview or Secure Webview.

Procedure 17-16 To configure Dying Gasp on an OS 6250 (Metro) NE

Note — In order to see the Dying Gasp alarm in the 5620 SAM, the NE must be managed using SNMP V2, with a "public" community string, since this alarm has a pre-defined community string of "public".

1 Use the 5620 SAM navigation tree; perform the following steps.

2 Choose Equipment from the view selector.

3 Right-click on an OS 6250 (Metro) icon.

4 Choose NE Sessions→*option* from the contextual menu

where *option* is Telnet Session or SSH Session

5 Choose Telnet Session.

6 The Telnet Session window opens.

7 See Step 5 of Procedure 13-4 to configure the NE to be managed with a "public" community string using SNMP v2.

Note 1 — If the Backup/Primary power supply fails, a major alarm will be raised. This alarm will be sent only to the first two SNMP stations configured on the NE. “Show snmp station” lists the management station address. SAM ip should be first or second.

Note 2 — The "Loopback 0" address should not be used for the source IP address field on the NE.

Procedure 17-17 To configure port/queue statistics on an OS 6250 port

This procedure provides port/queue statistics on an OS 6250 (Metro) or OS 6250 (SME) NE.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the OS 6250 device where you want to configure port and queue statistics and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Statistics tab button.

7 In the Select Object Type area, choose Qos Port/Queue Stats (Physical Equipment) from the contextual menu.

8 Click on the Collect button.

9 A statistics record appears on the Physical Port (Edit) form. Select the record.

10 Click on the Properties button. The Statistics Record - QoS Port/Queue Stats form opens.

11 View the read-only port/queue statistics parameter values for the OS 6250 port.

12 Click on the Close button. The Statistics Record - QoS Port/Queue Stats form closes.

13 Close the Physical Port (Edit) form.

Procedure 17-18 To configure Ip statistics on an OmniSwitch routing instance

This procedure provides Ip traffic statistics (received or transmitted) on a routing instance of an OmniSwitch.

1. Choose Routing from the view selector in the navigation tree. The navigation tree displays the Routing view.
2. Right-click on a Routing Instance in the Routing view and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with General tab displayed.
3. Click on the Statistics tab button.
4. In the Select Object Type area, choose Ip Traffic Stats (Received) (Routing Management General) or Ip Traffic Stats (Transmitted) (Routing Management General) from the contextual menu.
5. Click on the Collect button.
6. A statistics record appears on the Routing Instance (Edit) form. Select the record.
7. Click on the Properties button. The Statistics Record - IP Stats (Received) or Statistics Record - IP Stats (Transmitted) form opens, depending on which object is selected in Step 4.
8. View the read-only IP statistics parameter values for the OmniSwitch routing instance.
9. Click on the Close button. The Statistics Record - IP Stats (Received) or Statistics Record - IP Stats (Transmitted) form closes.
10. Close the Routing Instance (Edit) form.

17.6 Ring group configuration procedures

Use the following procedures to manage ring groups using the navigation tree.

Procedure 17-19 To create a ring group

You can use the ring group creation function to:

- indicate a VLAN ring topology, for example, by grouping 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices with 7450 ESSs that operate in the same spanning tree or Ethernet ring
- indicate a VPLS ring topology, for example by grouping 7250 SAS-ES and 7250 SAS-ESA devices with 7450 ESS, 7750 SR, and 7710 SR devices
- configure the properties of the ring group to provide VLAN Internet, BTV (MVR), and L2 VPN (TLS) services
- group devices by geographic region

Consider the following before you create a ring group.

- Ensure that the devices are commissioned, as described in chapter 13.
- Ensure that mediation policies are configured to allow CLI access to the managed devices, as described in chapter 14.
- The VLAN ID for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices must be unique in a ring group.
- If you want specific access interfaces to be part of a VLAN service, ensure that the parent device of the interface is a member of the ring group.

1 Choose Ring Group from the view selector in the navigation tree. The navigation tree displays the Ring Group view.

2 Right-click on the Network object and choose Create Ring Group from the contextual menu. The Ring Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Ring Group Type

4 Click on the Apply button.

5 If you set the Ring Group Type parameter to VPLS in step 3, go to step 8.

6 Click on the TLS tab button to configure L2 VPN parameters.

7 Configure the TLS parameters:

- Enabled
- Ethertype
- Jumbo Frame

The Ethertype and Jumbo Frame parameters are configurable when the Enabled parameter is selected.

8 Perform one of the following to add a device to the ring group.

a Perform the following steps to use the current properties form.

i Click on the Group Members tab button.

ii Click on the Create button. The Select Network Elements form opens.

iii Choose one or more NEs and click on the OK button. A dialog box appears.

iv Click on the OK button. The Select Network Elements form closes and the selected devices are listed on the Ring Group (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The Ring Group (Edit) form closes and the device objects are listed in the navigation tree under the new ring group object.

b Perform the following steps to use the navigation tree.

i Right-click on the device object in the Equipment view of the navigation tree and choose Add To Ring Group from the contextual menu. The Select Group form opens to display a list of ring groups.

ii Choose the new ring group and click on the OK button. The Select Group form closes and the device object is listed under the ring group in the Ring Group view of the navigation tree.

Note — All device types can be added as members of a VLAN ring group. Only devices that support VPLS can be added to a VPLS ring group.

9 To apply a span of control to a ring group, click on the Spans tab button.

i Click on the Add button. The Select Span(s) - Ring Groups form opens with a list of available spans.

ii Choose one or more spans of control to apply to the ring group.

iii Click on the OK button. The Select Span(s)-Ring Group form closes and a dialog box appears.

iv Click on the OK button.

10 To view network-level alarms from a 7250 SAS or other device in a ring group, click on the Faults tab button.

11 Provision VLAN services, as described in chapter 69.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Ring Group (Create) form closes.

Procedure 17-20 To remove a ring group or ring group device

1 Choose Ring Group from the view selector in the navigation tree. The navigation tree displays the Ring Group view.

2 Navigate to the required ring group object.

3 To remove a device from the ring group, right-click on the device object under the ring group and choose Remove From Ring Group from the contextual menu. The device is removed from the ring group.

4 To remove a ring group:

i Perform step 3 for each device in the ring group to remove all devices from the ring group.

ii Right-click on the Ring Group object and choose Remove Ring Group from the contextual menu. A dialog box appears.

iii Click on the Yes button. The ring group is removed.

Caution — Removing a ring group deletes the VLAN services that are associated with the ring group.

17.7 Circuit emulation configuration procedures

Use the following procedures to manage circuit emulation using the navigation tree.

Caution — Do not use the CLI to manage a CES on the 7250 SAS, Release 1.0 R3 or later. Doing so may result in database inconsistencies between the network element and the 5620 SAM.

Procedure 17-21 To configure a 7250 SAS CES module

Perform this procedure to configure CES on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA device.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES module and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the daughter card slot level and click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA daughter card slot object that accommodates a CES module, such as slot 4 or 5. The Daughter Card Slot (Edit) form opens with the General tab displayed.

5 Click on the CES tab button.

6 Configure the parameters:

- Mode
- IP Address
- Gateway IP Address
- Clock Mode
- Mask

7 Click on the OK button. A dialog box appears.

8 Click on the OK button.

Procedure 17-22 To configure a 7250 SAS CES port

Perform this procedure to configure the framing scheme for the attached E1 or T1 line on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA device.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the Default VLAN parameter.

7 Click on the States tab button.

8 Configure the Administrative State parameter.

9 Click on the T1/E1 tab button.

10 Configure the parameters:

- Port Framing
- Line Code
- Loopback
- Line Buildout
- Line Length
- Db Loss
- Line Impedance

The Db Loss parameter is configurable when the Line Buildout parameter is set to Long.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button.

Procedure 17-23 To create an unstructured CES interface on a 7250 SAS device

This procedure applies to 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA devices. Perform this procedure to create an unstructured CES interface on a TDM port to extend clear channel services across an Ethernet or MPLS network.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA unstructured CES interface and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level, right-click on a configured 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port and choose Create Interface. The Unstructured Interface (Create) form appears.

5 Configure the Description parameter.

6 Click on the CES tab button.

7 Configure the Interface ID parameter.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The unstructured CES interface appears in the navigation tree under the port of the daughter card.

Procedure 17-24 To create a structured CES interface on a 7250 SAS device

This procedure applies to 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA devices. Perform this procedure to configure a structured CES interface to channel multiple DS-0 channels to one or more multiple destinations across an Ethernet or MPLS network.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA structured CES interface and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the daughter card slot level and right-click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA daughter card slot object that accommodates a CES module, such as slot 4 or 5.

5 Choose Create CES Channel Group from the contextual menu. The CES Channel Group (Create) form appears with the General tab displayed.

6 Configure the Channel ID parameter.

Note — Channel groups with an ID that is greater than 30 must be created, modified, or deleted using a CLI session due to SNMP limitations on the device. See chapter 15 for more information about starting a CLI session.

7 Click on the Channel Group tab button.

8 Click on the Select button in the Port panel. The Select Port - CES Channel Group form appears.

9 Choose a port from the list and click on the OK button. The Select Port - CES Channel Group form closes and the selection appears in the Name field.

10 Configure the Time Slots panel. For a DS0 group from a T1, choose from 1 to 24. For a DS0 group from an E1, choose from 1 to 31.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The structured CES interface appears in the navigation tree under the CES channel group of the daughter card.

Procedure 17-25 To modify a CES interface on a 7250 SAS device

This procedure applies to 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA devices.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES interface and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the interface level and right-click on a configured CES Interface. The Unstructured Interface (Edit) form opens for a CES interface that is assigned to a TDM port, or the Structured Interface (Edit) form opens for a CES interface that is assigned to a channel group. The General tab is displayed.

5 Configure the Description parameter.

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the CES tab button.

9 Configure the parameters:

- Protocol
- Max Jitter Expected (ms)
- Samples Aggregation
- Destination Port
- Destination IP Address
- Local Port
- Destination MAC Address
- Destination ECID
- Local ECID
- Priority

10 Click on the OK button. A dialog box appears.

11 Click on the OK button.

18 — Logical group object configuration

18.1 Logical group object configuration overview

Logical group objects are children of the device object. They appear below the device object in the navigation tree. The following logical group objects are created automatically in the navigation tree after the device is discovered.

- CCAG
- ISA-AA Group
- ISA-Tunnel Group
- ISA-LNS Group
- ISA-NAT Group
- ISA-Video Group
- LAG
- IGH

Properties forms for logical group objects are accessed using the 5620 SAM navigation tree.

This chapter contains the procedures to configure logical group objects using the navigation tree. See chapter 4 for more information about using the navigation tree.

18.2 Working with CCAG objects

CCAGs are navigation tree objects located below device icons. CCAGs are configured manually using the CCAG object navigation tree menu and subsequent forms. For proper CCAG configuration, a VSM-CCA card must be present in the NE. In the navigation tree, a VSM-CCA card can be opened to show its ports. The ports are indicated by VSM Port x/y/z, which shows port type and the ID of the port.

You must configure the following in the CCAG configuration forms:

- General properties such as CCAG ID, Description, CCA Rate Enabled, CCA Rate, Access Adapt QoS, and Administrative State
- CCAG MDA Members which are compatible ports that can belong to a CCAG.

When you create a CCAG, the 5620 SAM creates virtual paths to be used as interconnections to bind services together. Two unidirectional paths are created: Alpha and Beta. For each path, three virtual ports are created: one for SAP-SAP connections, one for SAP-NET connections, and one for NET-SAP connections. The last two virtual ports are used to bind a service and a network interface together.

A maximum of eight cards can be added to a CCAG, with a maximum of eight CCAGs per NE.

18.3 Working with ISA-AA groups and ISA-AA partitions

ISA-AA groups are created to provide redundancy for application assurance capabilities when multiple ISA-AA MDAs are installed on an NE. ISA-AA redundancy protects against card failure and minimizes service interruption during maintenance or protocol signature upgrades. When you create or delete an ISA-AA group, a default AA group policy is automatically created or deleted under the ISA-AA group.

You must configure the following on the ISA-AA groups configuration form:

- General properties, such as Group Number, Description, Operation Upon Failure, and Administrative State
- ISA-AA Group members
- ISA-AA Group diverted forwarding classes

An ISA-AA group can contain up to seven member ISA-AA MDAs, with up to seven ISA-AA groups per NE. Each group can contain up to seven primary members and one backup member.

ISA-AA groups are supported on the 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7, 7450 ESS-12, and 7750 MG.

The 5620 SAM supports ISA-AA partitions. Each partition is an object with its own AA policy. You can partition an AA group into AA policy partitions with one partition for each VPN-specific AA service. The partition support VPN-specific custom protocols, applications, application group definitions, policy definitions and reporting. Each partition policy can be divided into multiple application QoS policies using ASOs. Multiple ISA-AA groups are used to scale the number of VPN-specific AA policies.

See chapter 77 for information about ISA-AA partitions, AA groups, and AA policies. See Procedure 18-2 for information about how to create and configure ISA-AA partitions.

18.4 Working with ISA-Tunnel Groups

ISA-Tunnel Groups are created to provide redundancy for IP security tunneling and encryption functions when multiple ISA-IPSEC MDAs are installed on an NE. ISA-IPSEC redundancy protects against card failure and minimizes service interruption during maintenance or protocol signature upgrades.

You must configure the following in the ISA-Tunnel Groups configuration form:

- General properties, such as Group Number, Description, and Administrative State
- ISA-Tunnel group members

Up to two cards can be added to an ISA-Tunnel Group, with up to four ISA-Tunnel groups per NE. Each group can contain one primary and one backup member. One member is the active member.

18.5 Working with ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups. ISA-LNS groups provide LNS PPP session termination on 7750 SR NEs. You can assign an ISA-LNS group to a tunnel group profile or a tunnel profile. When an operational L2TP tunnel is established, peers that are associated with the ISA-LNS group are automatically created. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group. You can add ISA broadband application MDAs to an ISA-LNS group, and up to four ISA-LNS groups on each NE. See Procedure 18-7 for information about how to create and configure an ISA-LNS group.

You must configure the following on the ISA-LNS groups configuration form:

- General properties, such as Group Number, Description, and Administrative State
- ISA-LNS Group members

Note — You can configure an ISA broadband application MDA only on an IOM3-XP module in a Release 8.0 or later 7750 SR -7 or 7750 SR-12.

18.6 Working with ISA-NAT groups

An ISA-NAT group provides a redundant NAT function for routing instances using ISA Broadband Applications MDAs. An ISA-NAT group can contain up to six MDAs in a warm redundancy configuration. At least one member MDA must be in the active role for an ISA-NAT group to be operational. See chapter 30 for information about configuring the NAT function on a routing instance. See the NE documentation for more information about NAT deployment.

Note 1 — You can install an ISA-NAT Broadband Applications MDA in an IOM3-XP module.

Note 2 — The same ISA Broadband Applications MDA can belong to an ISA-NAT group and an ISA-LNS group.

Note 3 — ISA-NAT is supported on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher. See chapter 19 for information about chassis modes.

18.7 Working with ISA-Video groups

ISA-Video groups are created to provide packet buffering and packet processing in support of the IPTV video features.

When configured in the router, video ISAs are logically grouped into video groups. An ISA-Video group allows more than one video ISA to be treated as a single logical entity for a specific application, where the system performs a load-balancing function when it assigns tasks to a member of the group.

ISA-Video groups provide a redundancy mechanism to guard against hardware failure within a group. ISA-Video groups pool the processing capacity of all the group members and increase the application throughput because of the increased packet processing capability of the group.

You must configure the following on the ISA-Video groups configuration form:

- General parameters
- ISA-Video Group members

You can add up to four MDAs to an ISA-Video group, and up to four ISA-Video groups on each NE. All members of an ISA-Video group are primary members.

Note — If the parameter ad Insert server is enabled, only one MDA can be added to an ISA-Video group.

18.8 Working with IGH objects

IGHs are navigation tree objects located below the device icon. IGHs are configured manually using the configuration forms available when you choose Create IGH from the IGH object navigation tree contextual menu.

You create an IGH to group together IP links and POS links so that if a configured number of links go out of service for any reason, the remaining links in the IGH go out of service too. This causes the routing protocols to re-converge to switch from the primary path to an alternate path.

The following requirements and restrictions apply to IGHs.

- IGHs are supported only on network links.
- IGHs are supported only on SONET/TDM interfaces with PPP auto encapsulation.
- A port or channel needs to be bound to a router interface after the member is added to an IGH.
- You can assign a port to only one IGH.

18.9 Working with LAG objects

LAGs are navigation tree objects located below the device icon. LAGs are configured manually using the configuration forms available when you choose Create LAG from the LAG object navigation tree contextual menu.

The following minimum configuration is required to enable LACP.

- Enable LACP at either end of the LAG group.
- Set one end of the LAG group as LACP active.

You must configure the following in the LAG configuration forms:

- General properties, such as LAG description, configured address, encapsulation type, and administrative state
- Link aggregation group parameters, such as port threshold, port threshold action, and dynamic cost
- LACP parameters, such as LACP mode, LACP transmit interval, actor administration key, LACP transmission standby, and LACP selection criteria
- LAG members, which are the compatible ports that can belong to a LAG

Because all ports can have their own MAC address, when ports are part of a LAG, the LAG must have an MAC address.

The port configuration of the first port added to the LAG is used to compare with subsequently added ports. If a discrepancy is found with a newly added port, that port is not added to the LAG.

Up to 16 ports can be added to or removed from a LAG on IOM 3 and IMM cards in chassis mode D. Otherwise, up to only eight ports can be added to or removed from a LAG. All ports added to a LAG must have the same parameter settings.

Only ports belonging to one LAG subgroup are considered eligible members of a LAG and can be selected as active links.

See section 12.22 for OmniSwitch-specific LAG information.

See section 12.19 for 9500 MPR LAG information.

18.10 Workflow to manage logical group objects

The following workflow describes the sequence of high-level tasks required to manage and configure logical group objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — Logical group objects can be accessed using the equipment navigation tree. See chapter 4 for more information about using the equipment navigation tree.

1 As required, configure CCAG objects. See Procedure 18-1 for more information.

2 As required, create and configure ISA-AA groups and ISA-AA partitions. See Procedure 18-2 for more information. Additionally, perform the following, as required:

  a Configure QoS on an ISA-AA group. See Procedure 18-3 for more information.

  b Add a subscriber policy override to an ISA-AA group or ISA-AA partition. See Procedure 18-4 for more information.

  c Enable and configure Cflowd on an ISA-AA group and ISA-AA partition. See Procedure 18-5 for more information.

3 As required, configure ISA-Tunnel groups. See Procedure 18-6 for more information.

4 As required, configure ISA-LNS groups. See Procedure 18-7 for more information.

5 As required, create and configure ISA-NAT groups. See Procedure 18-8 for more information. Additionally, perform the following, as required:

   a Configure statistics on an ISA-NAT group. See Procedure 18-9 for more information.

   b Start or stop a NAT address-pool drain operation. See Procedure 18-10 for more information.

6 As required, configure ISA-Video groups. See Procedure 18-11 for more information.

7 As required, configure IGH objects. See Procedure 18-12 for more information.

8 As required, configure LAG objects:

   a Create and configure a LAG. See Procedures 18-13 and 18-14 for more information.

   b Create and configure a LAG on an OmniSwitch. See Procedure 18-15 for more information.

   c Create and configure a dynamic LAG member on an OmniSwitch. See Procedure 18-16 for more information.

   d Configure a Radio LAG or Ethernet LAG on the 9500 MPR. See Procedure 18-17 for more information.

   e Delete a 9500 MPR LAG member. See Procedure 18-18 for more information.

18.11 Logical group object configuration procedures

Use the following procedures to configure NE logical groups using the navigation tree.

Procedure 18-1 To create and configure a CCAG

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a CCAG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click the CCAGs icon and choose Create CCAG. The CCAG (Create) form opens with the General tab displayed.

5 Configure the parameters:

- CCAG ID
- Description
- CCA Rate Enabled
- CCA Rate (kbps)
- Access Adapt QoS
- Administrative State

6 Click on the CCAG MDA Members tab button to display and configure CCAG MDA members associated with this CCAG.

7 Click on the Create button. The CCAG MDA Member (Create) form opens.

8 Click on the Select button. The Select Member MDA - CCAG MDA Member form opens with a list of available VSM-CCA cards.

9 Choose the MDA to add to this CCAG and click the OK button. The Select Member MDA - CCAG MDA Member form closes and the CCAG MDA Member (Create) form reappears.

10 Click on the OK button. The CCAG MDA Member (Create) form closes.

11 Click on the CCAG Paths tab button. The Alpha and Beta paths are displayed. To modify a path, go to step 12. Otherwise, go to step 25.

12 Choose a path and click on the Properties button. The CCAG Internal Path (Edit) form opens with the General tab displayed.

13 Configure the parameters:

- Path Rate Enabled
- Path Rate (Kb/s)
- Path Rate Option
- Path Weight (%)

14 Click on the Path Cross Connects tab button. This tab displays the cross- connects associated with the path.

15 Choose a cross-connect to be configured and click Edit. The Cross Connect (Edit) form opens with the General tab displayed.

16 Configure the parameters:

- Description
- Configured MAC
- MTU (octets)

17 Click on the States tab button.

18 Configure the Administrative State.

19 Click on the Policies tab button.

20 To specify an egress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Egress Slope Policy panel.

ii Click on the Select button in the Egress Slope Policy panel. The Select Egress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Egress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

21 Configure the parameters:

- Committed Burst Size (%)
- Committed Burst Size (%)

22 To specify an ingress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Ingress Slope Policy panel.

ii Click on the Select button in the Ingress Slope Policy panel. The Select Ingress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Ingress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

23 Click on the OK button. The Cross Connect (Edit) form closes and the CCAG Internal Path (Edit) form reappears.

24 Click on the OK button. The CCAG Internal Path (Edit) form closes and the CCAG (Edit) form reappears.

25 Click on the OK button. The CCAG (Edit) form closes.

Procedure 18-2 To create and configure an ISA-AA group and ISA-AA partition

When you create or delete an ISA-AA partition, a default AA group partition policy and a default AA accounting policy are automatically created or deleted under the ISA-AA partition.

Note — An ISA-AA partition provides ISA-AA group functions but only in the context of the created partition. Application ID, policy, and statistics configuration apply only to the partition you created for the ISA-AA group.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an ISA-AA group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

Note — You can also create an ISA-AA group or ISA-AA partition from the Manage→ISA Functions→ISA-AA form.

4 Right-click on the ISA-AA Group icon and choose Create ISA-AA Group. The ISA-AA Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Operation Upon Failure
- Administrative State
- Partitions
- Subscriber Scale
- Overload Cut-Through
- Number of IPv4 Transit Prefix Entries
- Match All HTTP Requests
- HTTP X-Online-Host
- Capacity Cost High Threshold
- Capacity Cost Low Threshold

Note — If there are AA group policies on the ISA-AA group that you are configuring, you cannot modify the Partitions parameter from “Enabled” to “Disabled” or from “Disabled” to “Enabled.” Before you can modify the Partitions parameter, you must delete the AA group policies and the associated SAP dependencies.

6 If you set the Partitions parameter to Enabled, perform the following steps to create and configure an ISA-AA partition.

i Click on the ISA-AA Partitions tab button.

ii Click on the Create button. The ISA-AA Group Partition (Create) form opens.

iii Configure the parameters:

- Partition ID
- Description

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The ISA-AA Group (Edit) form appears with the ISA-AA partition listed.

vi If required, repeat step 6 to create another ISA-AA partition.

7 Specify a traffic forwarding class to divert to the ISA-AA group.

i Click on the ISA-AA Group Diverted FCs tab button.

ii Click on the Create button. The ISA-AA Group Diverted FC (Create) form opens.

iii Configure the Forwarding Class Name parameter.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The ISA-AA Group Diverted FC (Create) form closes.

8 Specify an ISA-AA MDA for the ISA-AA group.

i Click on the ISA-AA Group Members tab button.

ii Click on the Create button. The ISA-AA Group Member (Create) form opens.

iii Configure the ISA-AA MDA Role parameter.

iv Click on the Select button. The Select Member MDA - ISA-AA Group Member form opens with a list of available ISA-AA cards.

v Choose the MDA to add to this ISA-AA Group and click the OK button. The Select Member MDA - ISA-AA Group Member form closes and the ISA-AA MDA Member (Create) form reappears.

vi Click on the OK button. The ISA-AA Group Member (Create) form closes.

Note — The MDA slot number assigned to an AA subscriber or AA SAP on the AA Subscriber or AA SAP Summary form is displayed as Unassigned if the AA subscribers in the configuration file cannot fit after an NE reboot.

9 Perform Procedure 18-3 to specify the QoS parameters for the ISA-AA group.

10 Add a special-study subscriber to the ISA-AA group or ISA-AA group partition.

i Click on the AA Special Study tab button.

ii Click on the Subscribers tab button.

iii Click on the Create button. The AA Special Study Subscriber (Create) form opens.

iv Configure the parameters:

- AA Subscriber Name
- AA Stats Type

v Click on the OK button. The AA Special Study Subscriber (Create) form closes.

11 Add a special-study SAP to the ISA-AA group or ISA-AA partition.

i Click on the AA Special Study tab button.

ii Click on the SAPs tab button.

iii Click on the Add Per-SAP Protocols button to add a SAP for per-protocol monitoring, if required. The Select Per-SAP Protocols form opens. Otherwise, go to step 11 v.

iv Choose a SAP in the list and click on the OK button. The Select Per-SAP Protocols form closes and the SAP is listed on the AA Special Study SAPs tab.

v Click on the Add Per-SAP Applications button to add SAP for per-application monitoring, if required. The Select Per-SAP Applications form opens. Otherwise, go to step 12.

vi Choose a SAP in the list and click on the OK button. The Select Per-SAP Protocols form closes and the SAP is listed on the AA Special Study SAPs tab.

vii Click on the OK button. The AA Special Study Subscriber (Create) form closes.

12 Add AA objects for custom per-SAP or per-subscriber statistics collection.

i Click on the AA Subscriber Stats Objects tab button.

ii Click on the Add Applications button to add an application, if required. The Select Applications form opens.

iii Choose one or more applications in the list and click on the OK button. The Select Applications form closes and the applications are listed on the AA Subscriber Stats Objects tab.

iv Click on the Add Application Groups button to add an application group, if required. The Select Application Groups form opens.

v Choose one or more application groups in the list and click on the OK button. The Select Application Groups form closes and the application groups are listed on the AA Subscriber Stats Objects tab.

vi Click on the Add Protocols button to add a protocol, if required. The Select Protocols form opens.

vii Choose one or more protocols in the list and click on the OK button. The Select Protocols form closes and the protocols are listed on the AA Subscriber Stats Objects tab.

viii Click on the Add Custom Protocols button to add a custom protocol, if required. The Select Custom Protocols form opens.

ix Choose one or more custom protocols in the list and click on the OK button. The Select Custom Protocols form closes and the custom protocols are listed on the AA Subscriber Stats Objects tab.

13 Add special study spoke SDP bindings to the ISA-AA group or ISA-AA partition.

i Click on the AA Special Study tab button.

ii Click on the Spoke SDP Bindings tab button.

iii Click on the Add Per-Spoke SDP Binding Protocols button to add a per-spoke SDP binding protocol, if required. The Select Per-Spoke SDP Binding Protocol form opens.

iv Choose one or more protocols in the list and click on the OK button. The Select Per-Spoke SDP Binding Protocol form closes and the protocols are listed on the AA Special Study Spoke SDP Bindings form.

v Click on the Add Per-Spoke SDP Binding Applications button to add a per-spoke SDP binding application, if required. The Select Per-Spoke SDP Binding Applications form opens.

vi Choose one or more applications in the list and click on the OK button. The Select Per-Spoke SDP Binding Applications form closes and the applications are listed on the AA Special Study Spoke SDP Bindings form.

14 Add a special-study transit subscriber to the ISA-AA group or ISA-AA group partition.

i Click on the AA Special Study tab button.

ii Click on the Transit Subscribers tab button.

iii Click on the Create button. The AA Special Study Transit Subscriber (Create) form opens.

iv Configure the parameters:

- Transit Subscriber Name
- AA Stats Type

v Click on the OK button. The AA Special Study Transit Subscriber (Create) form closes.

15 Perform Procedure 18-4 to add an AA subscriber policy override to the ISA-AA group or ISA-AA partition.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button to apply the changes. The ISA-AA Group (Edit) form closes.

Procedure 18-3 To configure QoS on an ISA-AA group

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Right-click on the device where the desired ISA-AA group is created and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.
4. Expand the ISA-AA Groups icon.
5. Right-click on the desired ISA-AA Group and choose Properties. The ISA-AA Group (Edit) form opens.
6. Click on the QoS tab button.
7. Click on the Egress From-Subscriber tab button.
8. Configure the following parameters:

   Note 1 — You must deselect the Default check box before you can use the slider to specify values for the Reserved CBS (%) and the Buffer Utilization High Water Mark parameters.

   Note 2 — The value of the Buffer Utilization High Water Mark parameter must be higher than the value of the Buffer Utilization Low Water Mark parameter.

   - Reserved CBS (%)
   - Buffer Utilization High Water Mark
   - Buffer Utilization Low Water Mark
9. Click on the Select button in the Slope Policy panel. The Select Slope Policy form opens.
10. Choose a policy from the list and click on the OK button. The Select Slope Policy form closes.
11. Click on the Select button in the Network Queue Policy panel. The Select Network Queue Policy form opens.
12. Choose a policy from the list and click on the OK button. The Select Network Queue Policy form closes.
13. Click on the Select button in the Port Scheduler Policy panel. The Select Port Scheduler Policy form opens.
14. Choose a policy from the list and click on the OK button. The Select Port Scheduler Policy form closes.
15. Click on the Egress To-Subscriber tab button.

16 Configure the parameters:

Note 1 — You must deselect the Default check box before you can use the slider to specify values for the Reserved CBS (%) and the Buffer Utilization High Water Mark parameters.

Note 2 — The value of the Buffer Utilization High Water Mark parameter must be higher than the value of the Buffer Utilization Low Water Mark parameter.

- Reserved CBS (%)
- Buffer Utilization High Water Mark
- Buffer Utilization Low Water Mark

17 Click on the Select button in the Slope Policy panel. The Select Slope Policy form opens.

18 Choose a policy from the list and click on the OK button. The Select Slope Policy form closes.

19 Click on the Select button in the Network Queue Policy panel. The Select Network Queue Policy form opens.

20 Choose a policy from the list and click on the OK button. The Select Network Queue Policy form closes.

21 Click on the Select button in the Port Scheduler Policy panel. The Select Port Scheduler Policy form opens.

22 Choose a policy from the list and click on the OK button. The Select Port Scheduler Policy form closes and the ISA-AA Group (Edit) form appears.

23 Click on the OK button. A dialog box appears.

24 Click on the Yes button to apply the changes. The ISA-AA Group (Edit) form closes.

25 Close the Network Element (Edit) form.

Procedure 18-4 To add an AA subscriber policy override to an ISA-AA group or ISA-AA partition

The AA subscriber policy override is rejected if the subscriber does not have an application profile assigned. You can add an AA subscriber policy override to a SAP or Spoke SDP, but not to an ESM subscriber.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where the desired ISA-AA group is created and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-AA Groups icon.

5 Right-click on the desired ISA-AA Group and choose Properties. The ISA-AA Group (Edit) form opens.

6 Click on the AA Subscriber Policy Overrides tab button.

Note 1 — The AA subscriber policy override is rejected if the subscriber does not have an application profile assigned.

Note 2 — You can add an AA subscriber policy override to a SAP or Spoke SDP, but not to an ESM subscriber.

7 Click on the Create button. The AA Subscriber Policy Override (Create) form opens with the General tab displayed.

8 Configure the AA Subscriber Type parameter.

9 Perform one of the following:

a If you chose SAP, go to step 10.

b If you chose Spoke SDP Binding, go to step 12.

c If you chose Transit, go to step 14.

10 Click on the Select button in the SAP Subscriber panel. The Select SAP Subscriber - AA Subscriber Policy Override form opens.

11 Choose a SAP subscriber from the list and click on the OK button. The Select SAP Subscriber - AA Subscriber Policy Override form closes and the AA Subscriber Policy Override (Create) form refreshes with the SAP subscriber. Go to step 16.

12 Click on the Select button in the Spoke SDP Binding Subscriber panel. The Select Spoke SDP Binding Subscriber - AA Subscriber Policy Override form opens.

13 Choose a Spoke SDP Binding Subscriber in the list and click on the OK button. The Select Spoke SDP Binding Subscriber - AA Subscriber Policy Override form closes and the AA Subscriber Policy Override (Create) form refreshes with the Spoke SDP Binding name. Go to step 16.

14 Click on the Select button in the Transit Subscriber panel. The Select Transit Subscriber - AA Subscriber Policy Override form opens.

15 Choose a transit subscriber from the list and click on the OK button. The Select Transit Subscriber - AA Subscriber Policy Override form closes and the AA Subscriber Policy Override (Create) form refreshes with the transit subscriber.

16 Click on the ASO Characteristics tab button.

17 Click on the Create button. The AA Subscriber Policy Override ASO Characteristic (Create) form opens.

18 Click on the Select button beside the Override ASO Characteristic Name parameter. The Select Application Service Option form opens.

19 Choose an Application Service Option from the list and click on the OK button. The AA Subscriber Policy Override ASO Characteristic form refreshes with the ASO Characteristic Name.

20 Click on the Select button beside the Override ASO Characteristic Value parameter. The Select Application Service Option Characteristic Value form opens.

21 Choose an ASO Characteristic Value from the list and click on the OK button. The AA Subscriber Policy Override ASO Characteristic form refreshes with the ASO Characteristic Value.

22 Click on the OK button. The AA Subscriber Policy Override ASO Characteristic (Create) form closes and the AA Subscriber Policy Override (Create) form appears.

23 Click on the OK button. The AA Subscriber Policy Override (Create) form closes and the ISA-AA Group (Edit) form appears.

24 Click on the OK button. A dialog box appears.

25 Click on the Yes button to apply the changes. The ISA-AA Group (Edit) form closes.

26 Close the Network Element (Edit) form.

Procedure 18-5 To enable and configure Cflowd on an ISA-AA group or ISA-AA partition

Note — Before you perform this procedure, you must first enable global Cflowd on the NE. See Procedure 17-4 in chapter 17 for more information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device that contains the ISA-AA group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-AA Group icon and click on the ISA-AA group on which you are configuring Cflowd. The ISA-AA Group (Edit) form opens.

5 If you are configuring Cflowd on an ISA-AA partition click the ISA-AA Partitions tab button. Otherwise go to step 7.

6 Select a partition from the list and click Properties. The ISA-AA Group Partition (Edit) form opens.

7 Click on the CFLOWD tab button. The General tab is displayed.

8 Configure the remaining parameters:

- Sampling Rate
- Volume Administrative State
- TCP Performance: Sample Flow Rate
- TCP Performance: Performance Administrative State
- RTP Performance: Sample Flow Rate
- RTP Performance: Performance Administrative State
- Template Re-transmit
- Administrative State

If you are configuring Cflowd on an ISA-AA partition, only the Volume Administrative State, TCP Performance: Performance Administrative State, and RTP Performance: Performance Administrative State parameters in this list are configurable.

9 If you are configuring Cflowd on an ISA-AA partition go to step 13.

10 Click on the Collector tab button.

11 Perform the following steps to add a collector.

i Click on the Create button. The Cflowd Collector (Create) form opens.

ii Configure the parameters:

- Host Address
- Collector Port
- Description
- Administrative State
- Version

iii Click on the OK button. The CFLOWD Collector (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the ISA-AA group properties form.

12 Repeat step 11 to add another collector, if required.

Note — A Cflowd configuration on an ISA-AA group can contain a maximum of two collectors.

13 To add an AA application or AA application group for Cflowd performance monitoring, click on the Performance tab button. Otherwise, go to step 17.

14 Perform the following steps to add one or more applications, if required.

i Click on the Add Applications RTP or Add Applications TCP button. The Select Applications form opens.

ii Choose one or more applications in the list and click on the OK button. The Select Applications form closes, and the applications are listed on the ISA-AA group properties form.

15 Perform the following steps to add one or more application groups, if required.

   i Click on the Add Application Groups RTP or Add Application Groups TCP button. The Select Application Groups form opens.

   ii Choose one or more applications in the list and click on the OK button. The Select Applications form closes, and the applications are listed on the ISA-AA group properties form.

16 If you are configuring Cflowd on an ISA-AA partition, click OK to close the ISA-AA Group Partition (Edit) form.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The NE properties form closes.

Procedure 18-6 To create and configure an ISA-Tunnel group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an ISA-Tunnel group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the ISA-Tunnel Group icon and choose Create ISA-Tunnel Group. The ISA-Tunnel Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Administrative State

6 Click on the Apply button.

7 Click on the ISA Tunnel Group Members tab button.

8 Click on the Create button. The ISA Group Member (Create) form opens.

9 Click on the Select button. The Select Daughter Card - ISA Group Member form opens with a list of available ISA IPsec cards.

10 Choose the MDA to add to this ISA-Tunnel group and click the OK button. The Select Daughter Card - ISA Tunnel Group Member form closes and the ISA Group Member (Create) form reappears.

11 Click on the OK button. The ISA Group Member (Create) form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Tunnel Group form closes.

14 Repeat steps 4 to 13 to configure the backup ISA-Tunnel group member.

Procedure 18-7 To create and configure an ISA-LNS group

Perform this procedure to create and configure an ISA-LNS group. You can configure an IES or VPRN group interface to terminate LNS PPP sessions. See chapter 73 for information about configuring an IES group interface. See chapter 74 for information about configuring a VPRN group interface.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an ISA-LNS group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the ISA-LNS Groups icon and choose Create ISA-LNS Group. The ISA-LNS Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Administrative State

6 Click on the Apply button. The ISA-LNS Group (Edit) form opens with the General tab displayed.

7 Click on the ISA-LNS Group Members tab button.

8 Click on the Create button. The ISA-LNS Group Member (Create) form opens with the General tab displayed.

Note — You can configure up to six ISA-LNS group members. For each group member, you must choose an ISA Broadband Applications MDA. An ISA Broadband Applications MDA can be configured only on an IOM3-XP module on a 7750 SR.

9 Click on the Select button. The Select Member MDA - ISA-LNS Group Member form opens with a list of available ISA broadband applications cards.

10 Choose the MDA to add to the ISA-LNS Group and click the OK button. The Select Member MDA - ISA-LNS Group Member form closes and the ISA-LNS Group Member (Create) form reappears. The Slot Name field displays your selection.

11 Click on the OK button. The ISA-LNS Group Member (Create) form closes.

12 Repeat steps 4 to 11 to configure another ISA-LNS Group member, if required.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The ISA-LNS Group Member (Create) form closes.

Procedure 18-8 To create and configure an ISA-NAT group

Perform this procedure to create and configure an ISA-NAT group. See chapter 30 for information about configuring the NAT function on a routing instance.

Note — You can create an ISA-NAT group only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher. See chapter 16 for information about chassis modes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an ISA-NAT group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the ISA-NAT Groups icon and choose Create ISA-NAT Group. The ISA-NAT Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Active MDA Limit
- Reservation Count
- Session Watermark High
- Session Watermark Low

6 Click on the Apply button. The ISA-NAT Group (Create) form refreshes with additional tabs, and the form name changes to ISA-NAT Group (Edit).

7 Click on the ISA-NAT Group Members tab button.

8 Click on the Create button. The MDA (Create) form opens.

Note — You can configure up to six ISA-NAT group members. Each group member must be an ISA Broadband Applications MDA.

9 Click on the Select button. The Select Daughter Card form opens.

10 Choose an MDA in the list and click the OK button. The Select Daughter Card form closes, and the MDA (Create) form displays the MDA identifier.

11 Click on the General tab button.

12 Configure the Administrative State parameter.

> **Note —** You can set the Administrative State parameter to Up only when the ISA-NAT group contains at least one member MDA and when the Active MDA Limit parameter is set to a value greater than 0.

13 Click on the OK button. The MDA (Create) form closes and a dialog box appears.

14 Click on the OK button. The ISA-NAT Group (Edit) form lists the member MDA.

15 Repeat steps 8 to 14 to configure another ISA-NAT group member, if required.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The ISA-NAT Group (Edit) form closes.

Procedure 18-9 To configure statistics on an ISA-NAT group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure statistics and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-NAT Groups icon and click on the ISA-NAT group on which you want to configure statistics. The ISA-NAT Group (Edit) form opens with the General tab displayed.

5 Click on the ISA-NAT Group Members tab button.

6 Click on the Search button. A list of ISA-NAT Group Members is displayed.

7 Select an ISA-NAT group member from the list and click on the Properties button. The ISA-NAT Group Member (Edit) form opens.

8 Click on the Statistics tab button.

9 In the Select Object Type area, choose Network Access Translation ISA Member Stats (Network Address Translation), Network Access Translation ISA Member Usage Stats (Network Address Translation), or Network Access Translation Policy Stats (Network Address Translation) from the contextual menu.

10 Click on the Collect button.

11 A statistics record appears on the ISA-NAT Group Member (Edit) form. Select the record.

12 Click on the Properties button. The Statistics Record form opens.

13 View the read-only statistics parameter values for the ISA-NAT group member.

14 Click on the Close button. The Statistics Record form closes.

15 Close the ISA-NAT Group Member (Edit) form.

16 Close the ISA-NAT Group (Edit) form.

Procedure 18-10 To start or stop a NAT address-pool drain operation

Perform this procedure to control the removal, or draining, of the host sessions associated with a NAT pool address range.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance that has one or more configured NAT pools. The path is Routing→NE→Routing Instance.

3 Right-click on the routing instance and click on the Properties button. The Routing Instance properties form opens.

4 Click on the NAT Configuration tab button.

5 Click on the Search button. A list of NAT configurations is displayed.

6 Choose the required NAT configuration in the list and click on the Properties button. The NAT Configuration (Edit) form opens with the General tab displayed.

7 Click on the NAT Pools tab button.

8 Click on the Search button. A list of address pools is displayed.

9 Choose the required address pool in the list and click on the Properties button. The NAT Pool (Edit) form opens.

Note — You can also select multiple address pools and use the Drain or Stop Drain buttons to control the draining for the selected address pools, as described in subsequent procedure steps.

10 To start a drain operation on the address pool, click on the Drain button. The number of host sessions associated with the address range decreases as sessions close.

11 To stop an active drain operation on the address pool, click on the Stop Drain button. New host sessions are allowed to use the address range.

12 Close the open forms, as required.

Procedure 18-11 To create and configure an ISA-Video group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to create an ISA-Video group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the ISA-Video Group icon and choose Create ISA-Video Group. The ISA-Video Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Administrative State
- Local Retransmission Server
- Fast Channel Change Server
- Ad Insert Server
- Reserve Retransmission Bandwidth (Mbps)
- Stream Selection
- Analyzer

6 Click on the Apply button. The form displays four additional tabs.

7 Click on the Video Group Members tab button.

8 Click on the Create button. The Video Group Member (Create) form opens.

9 Click on the Select button. The Select Daughter Card - Video Group Member form opens with a list of available ISA Video cards.

10 Choose the MDA to add to this Video Group and click the OK button. The Select Daughter Card - Video Group Member form closes and the Video Group Member (Create) form reappears. The Slot Name field displays your selection.

11 Click on the OK button. The Video Group Member (Create) form closes.

12 Repeat steps 4 to 11 to configure another ISA-Video Group member, if required.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The ISA-Video Group (Create) form closes.

Procedure 18-12 To create an IGH and add members

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device on which to create an IGH and add members and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the IGH object and choose Create IGH from the contextual menu. The Create IGH form opens.

5 Configure the parameters:

- IGH ID
- Minimum Active Link Threshold
- Administrative State

6 Click on the Ok button. The Create IGH form closes.

7 Expand the IGH object and right-click on the IGH group object. Choose Create IGH Members from the contextual menu. The Create IGH Members form opens.

8 Click on the Select button beside the CLI Name parameter. The Select Port States - IGH Member form opens.

9 Choose a port from the list and click on the Ok button. The Create IGH Members form reappears.

10 Click on the OK button. The Create IGH Members form closes.

11 Repeat steps 9 and 10 to add more members, if required.

18.12 LAG configuration procedures

Use the following procedures to manage LAGs using the navigation tree.

Note — You cannot use the 5620 SAM to manage LAGs on the 7250 SAS.

Procedure 18-13 To create a LAG

Note — This procedure applies to 7210 SAS, 7450 ESS, 7710 SR, 7705 SAR and 7750 SR nodes. See Procedure 18-16 for information about how to configure a LAG on an OmniSwitch. See Procedure 18-17 about how to configure a LAG on a 9500 MPR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a LAG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Right-click on the LAGs object and choose Create LAG from the contextual menu. The Create LAG form opens.

5 Configure the parameters:

Note — The parameters that appear, and which can be configured, are dependant on the device type that the LAG is being configured for.

- LAG ID
- Auto-Assign ID
- Port Type
- Description
- Configured Address
- L2Uplink
- Mode
- Encap Type
- Administrative State

If you are creating a LAG for HSMDA, the Port Type parameter must be set to hsmda. The Encap Type must be either Dot1Q or Q in Q. Setting Mode to network creates a network LAG, and setting it to access creates an access LAG.

6 If you are configuring a LAG on a 7210 SAS-D 6F 4T ETR, 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, or 7210 SAS-M 24F 2XFP ETR, you can add the LAG to an SHG. See Procedure 20-16 in chapter 20 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the SHG name.

Note 1 — A LAG cannot be added to or deleted from an SHG if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one SHG; you must remove all SHGs from the LAG before you can add the LAG to a different SHG.

7 If you are configuring a LAG on a 7210 SAS-D 6F 4T ETR or 7210 SAS-E, go to step 12.

8 Click on the Next button. The Configure LAG Parameters form opens.

9 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

10 Click on the Next button.

a If you set the Mode parameter in step 5 to Access, the Configure Access Parameters form opens. Go to step 11.

b If you set the Mode parameter in step 5 to Network, the Configure LACP form opens. Go to step 13.

11 Configure the QoS Adaptation and Enable Per Forwarding Path Ingress Queue parameters.

Note — If you are creating a LAG for HSMDA, the QoS Adaptation parameter must be set to Link, otherwise the LAG will not be created.

12 Click on the Next button. The Configure LACP form opens.

13 Configure the parameters:

Note — The availability of configurable parameters depends on the node type for which the LAG is being configured.

- LACP Enabled
- Standby Signalling
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP System ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

Note 1 — The LACP Enabled parameter must be enabled before you can configure LACP and select a subgroup as an active subgroup.

Note 2 — The LACP Mode, LACP Transmit Interval, Actor Administration Key, LACP System ID, and LACP System Priority parameters are configurable when the LACP Enabled parameter is enabled.

14 Click on the Next button. The Configure LAG Members form opens.

15 Click on the Create button to add network ports to LAGs. The Only show compatible ports form appears.

16 Configure the Show Only Compatible Ports and Class parameters.

17 Click on the Next button. The Select Ports form opens.

18 Choose compatible ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose one or more ports—up to two if you are configuring a 7210 SAS-E, and up to four if you are configuring a 7210 SAS-D 6F 4T ETR, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, or 7210 SAS-M 24F 2XFP ETR.
- Click on the Next button. The Specify the Member Properties form opens.

Note 1 — For ports to appear as compatible ports, ensure no SAPs or services are configured on them.

Note 2 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 3 — For HSMDAv2 ports in a LAG, you must set the Auto-Negotiate parameter to False or Limited. Refer to Procedure 20-1 in chapter 20 for more information on configuring Ethernet ports.

Note 4 — You must use the same load balance algorithm for the ports associated with the LAG.

19 Configure the parameters:

- Priority
- Sub-Group ID

20 If required, perform step 36 of Procedure 20-1 to add Egress Secondary Shapers to a port member of an HSMDA LAG. The following devices support this function:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7450 ESS-6, Release 7.0 R3 or later
- 7450 ESS-7, Release 7.0 R3 or later
- 7450 ESS-12, Release 7.0 R3 or later
- 7750 SR-7, Release 7.0 R3 or later
- 7750 SR-12, Release 7.0 R3 or later

Note 1 — The add/delete/modify functions for Egress Secondary Shapers apply only to the primary port.

Note 2 — There can be a total of 64 egress secondary shapers per MDA, including the default shaper.

Note 3 — The Egress Secondary Shapers on the primary port of the LAG are propagated to each non-primary port member of the LAG, with a maximum 8 ports per LAG. These propagated shapers cannot be deleted.

For adding any new port to the LAG, the user must configure each Egress Secondary Shaper as per the primary port, otherwise the addition of the port is blocked.

Note 4 — When adding a port member to a LAG, the primary port and each selected port (maximum 8 ports) secondary shapers must have the same name and rate.

Ports with Egress Secondary Shapers cannot be added to a configured LAG which do not match the Egress Secondary Shapers of the primary port.

Note 5 — Shapers are not removed from the port when the port is removed from a LAG.

Note 6 — The SAP reference to the Egress Secondary Shapers within a LAG is supported. Only the primary port of the SAP on the LAG is used to determine the list of Egress Secondary Shapers for the SAP.

When port members are removed from the LAG, care must be taken to ensure that the last port member is not removed if the LAG is referenced to a SAP. Shapers must exist on a LAG to be referenced on a SAP. See chapters 64 to 76 for more information.

21 Click on the Finish button. The Specify Member Properties form closes and the Configure LAG Members form reappears. A dialog box appears.

22 Click on the OK button.

23 Click on the Finish button. The Configure LAG Members form closes and the Create LAG form reappears.

24 Click on the Close button.

25 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID, the LAG description and configured MAC address.
- The Link Aggregation Group tab displays the threshold parameters, cost information, and the primary port in the LAG, along with all the other LAG member ports.
- LAG member ports can be added from the LAG Members tab.
- Statistics, terminations, and fault information is available from the appropriate tabs.

26 Expand the LAG object in the navigation tree to view the created LAG groups. Expand the LAG group object to view the subgroup member ports, the priority, the subgroup ID, and the subgroup mode.

Procedure 18-14 To configure a LAG

Note — This procedure applies to 7210 SAS, 7450 ESS, 7710 SR, 7705 SAR and 7750 SR nodes. See Procedure 18-16 for information about how to configure a LAG on an OmniSwitch. See Procedure 18-17 for information about how to configure a LAG on a 9500 MPR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device that contains the LAG that you want to configure and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the LAGs icon and click on the LAG that you want to configure. The LAG (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Configured Address
- Mode
- OLC State

6 If you are configuring a LAG on a 7210 SAS you can add the LAG to an SHG. See Procedure 20-16 in chapter 20 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the SHG name.

Note 1 — A LAG cannot be added to or deleted from an SHG if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one SHG; you must remove all SHGs from the LAG before you can add the LAG to a different SHG.

7 If you are configuring a LAG on a 7210 SAS, go to step 12.

8 Click on the Link Aggregation Group tab button.

9 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

10 Click on the States tab button.

11 Configure the Administrative State parameter.

12 Click on the Access tab button.

13 Configure the parameters:

- QoS Adaptation
- Enable Per Forwarding Path Ingress Queue

Note — If you are configuring a LAG for HSMDA, the QoS Adaptation parameter must be set to Link.

14 Click on the LACP tab button.

15 Configure the parameters:

- LACP Enabled
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP System ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

The LACP Enabled parameter must be enabled before you can configure LACP and select a subgroup as an active subgroup.

The LACP Mode, LACP Transmit Interval, and Actor Administration Key parameters are configurable when the LACP Enabled parameter is enabled.

16 Click on the Next button. The Configure LAG Members form opens.

17 Click on the LAG Members tab. To add LAG members, perform steps 15 to 23 of Procedure 18-13.

18 If the LAG that you are configuring is in Network mode, the Network Interfaces tab is displayed. Click on the Create button. The Create Network Interface form opens. Perform steps 4 to 49 of Procedure 30-7 in chapter 30 to create a network interface. Otherwise go to step 22.

19 If the LAG that you are configuring is in Access mode or Hybrid mode and has an encapsulation type of dot1q or Q in Q, the MEPs tab is displayed. To add a facility MEP to the LAG, perform the following steps.

Note — Only one facility MEP can be configured on a LAG.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- CCM Messages Enabled
- Description
- CCM Messages Enabled
- Interface Type
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- Facility Fault Notify
- Facility VLAN ID

Note — To enable fault propagation on a facility LAG MEP, Facility Fault Notify must be enabled.

vi If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab button. Otherwise, go to step vii.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The MEP (Create) form closes.

20 To add a facility tunnel MEP to the LAG, perform the following steps.

Note — The LAG that you are configuring must be in Access mode or Hybrid mode and must have an encapsulation type of Q in Q.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- CCM Messages Enabled
- Description
- CCM Messages Enabled
- Interface Type
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- Facility Fault Notify
- Facility VLAN ID

Note 1 — To enable the fault propagation on a facility tunnel MEP, Facility Fault Notify must be enabled.

Note 2 — To link the facility tunnel status to the SAP, Facility VLAN ID must match the outer encapsulation value of the SAP.

Note 3 — To accept the fault notification from a facility MEP on the site where the SAP is located and on the SAP, Tunnel Fault Management must be set to Accept.

vi If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab button. Otherwise, go to step vii.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The MEP (Create) form closes.

21 To configure Ethernet-CFM redundancy on a facility MEP:

Note 1 — Ethernet-CFM redundancy must be configured on the node. See Procedure 17-2 for information. See chapter 80 for information about Ethernet-CFM redundancy.

Note 2 — The tunnel MEP must be part of an MC-LAG with Ethernet-CFM redundancy configured.

i Click on the MEPs tab button.

ii Click on the Search button. A list of MEPs is displayed.

iii Choose the facility MEP for which you need to configure Ethernet-CFM redundancy and click on the Properties button. The MEP (Edit) form opens.

iv Scroll to the Facility MEPS panel and select the Create Redundant MEP check box.

v Click on the OK button. The MEP (Edit) form closes. A redundant tunnel MEP with the same ID and Operational MAC address is created on the peer LAG. The redundant MEP has the same state as the MC-LAG in which that MEP resides.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The LAG (Edit) form closes.

Procedure 18-15 To create and configure an OmniSwitch LAG

Perform the following procedure to configure a static or dynamic LAG.

Workflow for a static LAG:

- create a static LAG on the local and remote switches
- assign ports to the LAG on the local and remote switches
- create a VLAN for the static LAG on the local and remote switches (optional)

Workflow for a dynamic LAG:

- create a dynamic LAG on the local (actor) and remote (partner) switches
- assign ports with the same actor administrative key (which allows them to be aggregated) to the local and remote LAG
- create a VLAN for the dynamic link aggregation group on the local and remote switch (optional)

Note 1 — You can configure MVRP fixed ports/LAGs, 802.1 Q ports/LAGs, aggregate ports/LAGs, and VLAN Stacking Network ports/LAGs.

Note 2 — When a port is assigned to a LAG member, you cannot modify the port properties using the 5620 SAM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the LAG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the LAGs icon, right-click on a LAG object and choose Create LAG from the contextual menu. The Create LAG - Define General Properties form opens.

5 Configure the parameters:

- LAG ID
- Auto-Assign ID
- Mode
- Administrative State
- Automatic VLAN Binding

The Automatic VLAN Binding parameter can only be configured for network LAGs.

6 Click on the Next button. The Create LAG - Configure LAG Parameters form opens.

7 Configure the parameters:

- Size
- Name
- Type

8 Perform one of the following:

a If you set the Type parameter to Static, go to step 15.

b If you set the Type parameter to Dynamic, go to step 9.

9 Click on the Next button. The Create LAG - Configure LACP form opens.

10 Configure the parameters:

- Actor Administration Key
- Actor System ID
- Partner System ID
- Actor System Priority
- Partner System Priority
- Partner Administration Key

11 Click on the Finish button. The Create LAG - Wizard Completed form opens.

12 Enable the View the newly created interface check box if you need to view the LAG properties.

13 Click on the Close button. The Create LAG form closes.

See Procedure 18-16 in this section for information about adding members to a dynamic LAG.

14 Go to step 25.

15 Click on the Next button. The Create LAG - Configure LAG Members form opens.

16 Click on the Create button to add ports to the LAG. The Create LAG Member - Only show compatible ports form appears.

17 Configure the Show Only Compatible Ports and Class parameters.

18 Click on the Next button. The Create LAG Member - Select Ports form opens.

19 Click on the Search button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
- Click on the Next button. The Specify the Member Properties form opens.

Note 1 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 2 — Mobile, UNI, and NNI ports cannot be members of a LAG.

Note 3 — Only network ports can be members of a network LAG and only access ports can be members of an access LAG.

20 Click on the Finish button. A dialog box appears.

21 Click on the OK button. The Create LAG - Configure LAG Members form displays the LAG members.

22 Click on the Finish button. The Create LAG - Wizard Completed form opens.

23 Enable the View the newly created interface check box if you need to view the LAG properties.

24 Click on the Close button to close the form.

25 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID and LAG description.
- The Link Aggregation Group tab displays the primary port in the LAG along with all the other LAG member ports.
- LACP parameters can be modified from the LACP tab.
- LAG member ports can be added from the LAG Members tab.
- A UNI policy can be applied to a LAG used as a SAP in a stacked VLAN from the Policies tab.
- An MVRP configuration and VLAN restriction can be applied to a LAG from the MVRP tab. If a port is a LAG member, you cannot modify parameters on the MVRP general tab on that physical port.
- Statistics, network interfaces, and fault information is available from the appropriate tabs.

26 Expand the LAG object in the navigation tree to view the created LAG groups and the unassigned dynamic LAG members group. Expand the LAG group object to view the subgroup member ports, the priority, and the LACP state. Expand the Unassigned Dynamic LAG Members group object to view dynamic LAG members that have not been assigned to a dynamic LAG group.

Procedure 18-16 To create and configure OmniSwitch dynamic LAG members

Perform the following procedure to add members to a dynamic LAG and modify existing dynamic LAG members.

Note 1 — LAG members are not added during the creation of the dynamic LAG, as they are with static LAGs. When a new dynamic LAG member is created it is placed into the Unassigned Dynamic LAG Members object. The new dynamic LAG members remain under the Unassigned Dynamic LAG Members object until the system identifies a LAG with matching properties. When an unassigned LAG member joins a LAG, the member is removed from the Unassigned Dynamic LAG Members object and added to the appropriate LAG object.

Note 2 — When a port is assigned to a LAG member, you cannot modify the port properties using the 5620 SAM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the LAG members and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4. Right-click on the Unassigned Dynamic LAG Members object and choose Create LAG Members from the contextual menu. The Create LAG Member - Only show compatible ports form appears.

5. Configure the Show Only Compatible Ports and Class parameters.

6. Click on the Next button. The Create LAG Member - Select Ports form opens.

7. Click on the Search button to display a list of compatible ports. Choose ports from the list to construct the LAG.

   Add ports to the LAG as follows:

   - Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
   - Click on the Next button. The Specify the Member Properties form opens.

   Note 1 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

   Note 2 — For all ports in an LAG, you must disable auto-negotiation, configure the same speed, and set the ports to full duplex. Mobile ports cannot be part of a LAG.

8. Configure the parameters:

   - Priority
   - System Id
   - System Priority
   - Admin Key
   - Admin State

9. Click on the Finish button. The Create LAG - Wizard Completed form opens.

10. Enable the View the newly created interface check box if you need to view the LAG properties.

11. Click on the Close button to close the form.

12. If you need to modify a dynamic LAG member, go to step 13.

13. Right click on a LAG member and choose Properties from the contextual menu.

14. The LAG Member (edit) form opens on the General tab.

15. Configure the Priority parameter in the LAG Member panel, if required.

16. Configure parameters in the Actor panel, if required.

   - System Id
   - System Priority
   - Admin Key
   - Admin State

17 Configure parameters in the Partner panel, if required.

- Admin Key
- Admin System Id
- Admin Port
- Admin System Priority
- Admin Port Priority
- Admin State

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to save your changes and close the form.

20 Click on the Close button to close the form.

Procedure 18-17 To configure a Radio LAG or Ethernet LAG on the 9500 MPR

Note — You cannot configure Radio LAG or Ethernet LAG on the 9500 MPR, Release 3.1 ANSI and ETSI. Only service creation and discovery are supported for Radio LAG Release 3.1.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the LAG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the LAGs icon, right-click on a LAG object and choose Create LAG from the contextual menu. The Create LAG - Define General Properties form opens.

5 Configure the parameters:

- LAG ID
- Auto-Assign ID

6 Click on the Next button. The Create LAG - Configure LAG Parameters form opens.

7 Configure the parameters:

- Name
- Lag Aggregation Type
    - Radio L1
    - Radio L2
    - Ethernet
- Size

8 Click on the Next button. The Create LAG - Configure LACP form opens.

9 Configure the parameters:

- Actor Administration Key
- LACP
    - Active
    - Passive
    - Disabled
- Timeout
    - Short
    - Long

Note — LACP and Timeout are applicable only to Ethernet Lag Aggregation Type.

10 Click on the Next button. The Create LAG - Configure LAG Members form opens.

11 Click on the Create button to add ports to the LAG. The Create LAG Member - Only show compatible ports form appears.

12 The Show Only Compatible Ports parameters does not apply to the 9500 MPR. The Class parameters depends on the Lag Aggregation Type selected in step 7.

13 Click on the Next button. The Create LAG Member - Select Ports form opens.

14 Click on the Search button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Note 1 — Mixed ports cannot be associated with a LAG, for example, MPT-HC, MPT-MC, MPT-HL or ODU. Before you associate a Radio port with a LAG the PPP-RF must be disabled.

Note 2 — The Radio LAG mode is always in network mode. By default, Ethernet LAG is in access mode and can be used as a SAP. If a physical link is created using Ethernet LAGs as the endpoints, the mode automatically changes from access to network mode.

If a physical link is created between MPR and non-MPR LAG ports, and the MPR LAG port must be used as a SAP, the user must change the mode to access. See step 20 for more information about how to manually change the mode.

Note 3 — An Ethernet member port with a physical link or protection cannot be added to a LAG. To add the port you must first delete the physical link and you can then add the port to the LAG. See chapter 5 for more information about how to delete a physical link.

Note 4 — For Fast Ethernet LAG, electrical ports cannot be grouped with the optical ports.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.

15 Click on the Finish button. A dialog box appears.

16 Click on the OK button. The Create LAG - Configure LAG Members form displays the LAG members.

17 Click on the Finish button. The Create LAG - Wizard Completed form opens.

18 Enable the View the newly created interface check box if you need to view the LAG properties.

19 Click on the Close button to close the form.

20 Use the LAG Properties contextual menu to view information about the created LAG or to modify LAG parameters. The LAG [Edit] form is displayed.

- The General tab displays the LAG ID and LAG description. For Radio LAG and Ethernet LAG select one the following Mode.
  - Access (Ethernet LAG only)
  - Network (Radio LAG only)
- The Link Aggregation Group tab displays the number of ports in the LAG along with all the other LAG member ports and the Lag Aggregation Type.
  - For Ethernet LAG, select Hash and Size from the drop-down menu.
  - For Radio LAG, select Size from the drop-down menu.
- LACP parameters can be modified from the LACP tab.
- LAG member ports can be added from the LAG Members tab. See steps 10 to 17.
- VLAN port configuration parameters can be modified from the VLAN Port Configuration tab.
- LAG state cannot be Down if a service is associated with the LAG. The Administrative State can be configured to Up in the States tab button, only if a minimum of one port is associated with a LAG.

21 Expand the LAG object in the navigation tree to view the created LAG groups and the unassigned dynamic LAG members group. Expand the LAG group object to view the subgroup member ports, the priority, and the LACP state. Expand the Unassigned Dynamic LAG Members group object to view dynamic LAG members that have not been assigned to a dynamic LAG group.

Procedure 18-18 To delete a 9500 MPR LAG

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Select the device where you want to delete the LAG.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the LAGs icon, right-click on a LAG object and choose Delete from the contextual menu. A dialog box is displayed.

5 Select Yes, to complete the deletion.

Note — A LAG can be deleted only if a member is not associated with the LAG. To delete the last member from a LAG, the Administrative State of the LAG must be set to Down. A LAG can be shutdown only when the LAG is not a part of any service or physical link.

Creating a 9500 MPR service over a VLAN path for Radio and Ethernet ports and LAGs

See Chapter 5 for more information about how to create a physical link between Ethernet LAGs.

See Chapter 70 to create a 9500 MPR Cpipe service and create a VLAN path. See Procedure 20-13 in chapter 20 to associate the Ethernet and Radio LAG service with a TDM port.

19 — Shelf object configuration

19.1 Shelf object configuration overview

In the equipment navigation tree, shelf objects are children of device objects. They appear below logical group objects in the navigation tree. Card slot objects are children of shelf objects, and as such appear below the shelf object in the navigation tree. Daughter card slot objects are created in the navigation tree as children of the card slot object, after the card slot object is configured. APS bundle objects appear below the shelf object and Bundle objects appear below daughter card objects that are configured as channelized MDAs.

This chapter contains the procedures to configure shelf, card slot, daughter card slot, and bundle objects using the navigation tree. See chapter 4 for more information about using the navigation tree. See chapter 40 for more information about APS bundles.

19.2 Working with shelf objects

Shelf objects represent the hardware that is configured on a shelf. When you choose the shelf object in the navigation tree and click on Properties in the contextual menu, you can view the states and conditions of the shelf including:

- general information
- fan tray state and speed
- power supply tray statuses
- LED statuses
- card slots
- hardware environment information
- timing
- statistics
- dry contacts
- faults
- port segregation
- software control module
- software bank information
- cross connects

The Display tab displays a graphical representation of the device's shelf and its equipment components, such as the empty card slots and the cards that are installed on the device. You can double-click on an object under this tab to open its Properties configuration form. Right-click on the object and you have full access to the contextual menus for the object and any child objects, for example the ports of a card (dynamic graphical representation only).

Note — When you display a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device, the element manager for the device launches. The 5620 SAM permits users to launch the Telco element manager from the client GUI. This functionality is provided as a convenience to users, and is not part of the 5620 SAM. Contact Telco Systems for more information or support. See the appropriate device user guide for more information.

See Procedure 20-26 in chapter 20 for information on configuring 9500 MPR port segregation.

Chassis modes

The chassis mode of a device indicates the minimum IOM or IMM card type that is initialized by the device and determines the scaling numbers and features that are available to the system. The chassis mode can be configured on the following device types:

- 7450 ESS-4, 7450 ESS-6, 7450 ESS-7, and 7450 ESS-12
- 7450 ESS-6v
- 7750 SR-7 and 7750 SR-12

See the appropriate device Release Notice for scaling information.

Tables 19-1 and 19-2 list the chassis modes that you can configure on each IOM and IMM card type for the supported devices.

Table 19-1 Chassis modes and 7750 SR IOM and IMM card compatibility

Card	Chassis mode	NE release
2 x 10-Gig MDA IOM	A	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B	
2 x 10-Gig MDA IOM 2	A, B, and C	
2 x XP MDA IOM 3	A, B, C, and D	
2 x XP MDA IOM 3, B	A, B, C, and D	9.0 R6 or later
4-Port 10 GE XFP IMM	A, B, C, and D	All supported releases
8-Port 10 GE XFP IMM		
48-Port GIGE SFP IMM		
48-Port GIGE SFP IMM, B		9.0 R6 or later
48-Port GIGE TX IMM		All supported releases
48-Port GIGE TX IMM, B		9.0 R6 or later
12-Port 10GE SFP IMM		8.0 R5 or later
1-Port 100GE CFM IMM		
3-Port 40GE QSFP possibly oversubscribed IMM		9.0 R4 or later

Table 19-2 Chassis modes and 7450 ESS IOM card compatibility

Card	Chassis mode	7450 ESS-7, 7450 ESS-12, and 7450 ESS-4	7450 ESS-6	7450 ESS-6v
2 x 10-Gig MDA IOM	A	All supported releases	All supported releases	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B			
2 x 10-Gig MDA Oversubscribed IOM	A and B			
2 x XP MDA IOM 3	A, B, and B	All supported releases	All supported releases	All supported releases
2 x XP MDA IOM 3, B	A, B, C, and D	9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
48-Port GIGE SFP IMM		All supported releases	All supported releases	All supported releases
48-Port GIGE SFP IMM, B		9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
48-Port GIGE TX IMM		All supported releases	All supported releases	All supported releases
48-Port GIGE TX IMM, B		9.0 R6 or later	9.0 R6 or later	9.0 R6 or later
3-Port 40GE QSFP possibly oversubscribed IMM		9.0 R4 or later	—	—

Timing synchronization

Timing synchronization parameters can be configured on 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, 7750 SR-c4, and 7750 SR-c12 shelves that contain the following daughter cards:

- 10 Gigabit Ethernet with 2- and 4-port configurations
- 10/100/1000 Ethernet SFP with 20 ports
- 10 Gigabit Ethernet XFP with 4-, 8-, and 48-port configurations
- 10-port Gigabit Ethernet SFP HA
- 16 x Channelized DS1/E1 ASAP
- 16 x Channelized DS1/E1 ASAP v2
- 8-port Ethernet
- 8-port Ethernet v2
- 4-port OC3/STM1 ASAP SFP

See Procedure 19-5 for more information about configuring timing synchronization.

IEEE 1588 PTP clock

The IEEE 1588 PTP clock allows you to synchronize NE times with up to three reference points. The 5620 SAM supports IEEE 1588 PTP clocks on the 7450 ESS, 7705 SAR, 7705 SAR-M/ME, 7710 SR, 7750 SR, 7750 SR-c4, and 7750 SR-c12. Each NE can be configured with an ordinary master, ordinary slave or boundary clock. The 7705 SAR-M/ME can also be configured with a transparent clock.

19.3 Working with card and card slot objects

When you click on the plus sign beside the shelf object, all the card slots contained in the shelf appear in the navigation tree. They can appear as empty card slots when a card is not provisioned for the slot. Card slot objects for the OS 6250, OS 6400, OS 6850, OS 6850E, and OS 6855 appear automatically when a physical device exists because the entire device is represented by a card slot object, because there are no daughter cards associated with these devices. Card slots can be configured with CMM or Ethernet card types for the OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E devices, but there are no daughter cards associated with these devices.

When the 5620 SAM discovers a 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP, or 7705 SAR-F, the integrated IOM and daughter card objects appear automatically in the navigation tree.

Card slot objects for the 9500 MPR can be configured for plug-in cards; there are no daughter cards associated with this device.

Choose Configure Card from the contextual menu of the object and assign a supported card type for the slot. The Assigned Card Type parameter lists the card types can be assigned to the card slots.

Some card types can be pre-provisioned in a slot before the card is installed in the chassis. A card and daughter card must be provisioned before a port can be configured.

When a card is first configured, the administrative state can be down. The resource is not operationally up until the card is equipped and the administrative state is up. A card can only be provisioned in a slot that is vacant, and no other card can be provisioned (configured) for that specific slot.

To reconfigure a slot position, delete the card currently in the slot and configure the new card type added to the slot. A card can only be provisioned in a slot when the card type is allowed in the slot.

Note — You can also reconfigure a slot position by changing the chassis mode. The chassis mode determines the minimum card requirements. See section 19.2 for more information about chassis modes.

For example, if a 2 x 10-Gig MDA IOM 2 card is installed in the chassis that is running in chassis mode B, the card behaves as a 2 x 10-Gig MDA IOM Card, B. You can upgrade the chassis mode to C to make the IOM card behave as a 2 x 10-Gig MDA IOM 2 card.

Card provisioning and chassis modes

The behavior of the installed card depends on the chassis mode that has been configured on the device. Table 19-3 describes the behavior of the provisioned (configured) card types and installed cards in each chassis mode.

Table 19-3 Behavior of installed IOM cards

Provisioned card type	Installed card type	Behavior
2 x 10-Gig MDA IOM	2 x 10-Gig MDA IOM	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM Card, B is fully backward-compatible with the 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM.
	2 x XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x XP MDA IOM is fully backward-compatible with the 10-Gig MDA IOM.
2 x 10-Gig MDA IOM Card, B	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM Card, B.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
	2 x XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x XP MDA IOM 3 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
2 x 10-Gig MDA IOM 2	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D
	2 x XP MDA IOM 3 (1)	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D

(1 of 2)

Provisioned card type	Installed card type	Behavior
2 x XP MDA IOM 3 card [(1)]	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The IOM card fails because the minimum card requirements are not met.
	2 x XP MDA IOM 3 [(1)]	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C • 2 x XP MDA IOM 3 in chassis mode D. With mixed mode enabled for 7750 SR, only the IPv6 features of the IOM3 card are enabled, but no other IOM3 features are available.
2 x XP MDA IOM 3, B card [(1)]	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The IOM card fails because the minimum card requirements are not met.
	2 x XP MDA IOM 3 [(1)]	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C • 2 x XP MDA IOM 3 in chassis mode D. With mixed mode enabled for 7750 SR, only the IPv6 features of the IOM3 card are enabled, but no other IOM3 features are available.

(2 of 2)

Note

(1) Also applies to any IMM

19.4 Working with daughter card objects

After the card is created in the card slot you can create and configure MDAs, also known as daughter card objects, in the daughter card slot that appears when you click on the plus sign beside the card object. The daughter card slots in the card appear in the navigation tree. They appear as empty daughter card slots when a daughter card is not provisioned for the slot. When a daughter card is provisioned for the slot, it is identified.

See the appropriate device section in chapter 12 for device-specific daughter card information.

Each 5620 SAM license key allows a specific number of MDA cards of each node type to be managed. You can purchase additional MDA management capacity as required. MDA cards fall into two licensing categories: premium and standard. Generally, all non high performance MDA cards are considered standard. All IMM, High Speed MDA (HSMDA) and Extended Performance (XP) MDA cards are considered premium.

Note 1 — When the 5620 SAM has discovered the number of premium MDAs allowed by the license key, the 5620 SAM can no longer discover 7210 SAS-M, 7210 SAS-X, 7710 SR, and 7450 ESS devices.

Note 2 — Upgrading the 5620 SAM to a new major release may require adjustment to the license keys to avoid license keys warnings with exception MDA cards. See the appropriate *5620 SAM Release Description* for information about which exception MDA cards have been downgraded.

IMM daughter cards

The IMM card integrates IOM 3 and high bandwidth MDA functionality on a single card that fits into existing IOM slots. When you configure the IMM the integrated MDAs are automatically configured. The 5620 SAM equipment tree displays the IMM with two daughter cards, each having half of the total number of ports supported by the IMM.

Each daughter card object contains a number of ports that are specific to the type of service required. The port objects are created automatically under the daughter card but they must be configured based on the function served by the port; for example, as an access interface for a VPRN service.

You can associate policies to daughter cards. Network buffer policies are used to create and edit QoS buffer pool resources on egress network ports, channels, and ingress ports. Ingress and egress network ports and channels have a dedicated buffer pool for egress queuing. The ingress and egress network traffic is handled by a buffer pool at the ingress and a buffer pool at the egress.

You can also configure multicast path management on an IMM daughter card. See chapter 49 for more information.

MDA modes for the 7705 SAR

The 5620 SAM allows you to configure the MDA mode of some MDA types on the 7705 SAR. The MDA mode on a channelized ASAP determines the capabilities that are available to the MDA. The MDA mode on an XMDA determines the number of ports that are available to the MDA. See the MDA Mode parameter description for more information.

19.5 Working with bundle objects

Bundle objects can be configured as multilink PPP, IMA group, or FR group bundles. Multilink PPP, IMA group, and FR group bundles appear as Bundle objects under the daughter card object if the daughter card has been configured as a channelized MDA.

APS Bundle objects appear in the navigation tree as children of the shelf object. APS Bundle objects are configured to protect multilink PPP and IMA bundles on channelized ASAP MDAs. See chapter 40 for more information on APS and APS bundles.

Multilink PPP bundles

You can create multilink PPP bundles to:

- bundle DS0 channels together to be used as a SAP
- provide a mechanism to distribute data across multiple links to achieve higher bandwidth

The following general rules apply to multilink bundles.

- Table 19-4 lists the maximum number of multilink bundles that can be created on each MDA.
- DS0 channels can be aggregated on a single MDA only.
- Up to 8 members can be added to a bundle.
- The Encap Type parameter of a member cannot be set to FR.
- A DS0 channel can host only one SAP.
- If a channel is being used as a SAP, it cannot be added to a bundle.

Table 19-4 Multilink bundle configuration maximum

MDA	Bundle maximum
All MDAs other than channelized ASAP MDAs	56
• 1 x OC12 Deep Channel • 4 x OC3 Deep Channel • 12 x DS3/E3 Deep Channel • 4 x DS3/E3 Deep Channel • 8 x DS1/E1 Channel CMA (7710 SR)	56
4 x Channelized DS3/E3 ASAP MDA	112
• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP	256

See Procedure 19-28 to create a multilink PPP bundle.

IMA group bundles

IMA group bundles combine ATM-encapsulated DS0 channel groups into a single ATM interface. The following general rules apply to IMA group bundles.

- IMA group bundles can only be created on:
  - channelized ASAP MDAs with SDH or SONET framing the 7750 SR or 7710 SR
  - ATM DS1/E1 CMA on the 7710 SR
  - channelized DS1/E1 ASAP daughter cards on the 7705 SAR
- The encapsulation type of the DS0 group channel must be ATM.

- The Clock Source parameter of the DS1 channel must be set to Node-Timed.
- Table 19-5 lists the maximum number of IMA group bundles that can be created on each MDA.
- IMA group members must be on the same MDA.

Table 19-5 IMA group bundle configuration maximums

Device	MDA	Bundle maximum
7750 SR, all supported releases	All MDAs other than channelized ASAP MDAs	56
7750 SR, all supported releases 7710 SR, all supported releases	4 x Channelized DS3/E3 ASAP MDA	112
7750 SR, all supported releases 7710 SR, all supported releases	• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP	256
7710 SR, all supported releases	8 x ATM DS1/E1 CMA	8
7705 SAR, all supported releases	16 x Channelized DS1/E1 ASAP	8
7705 SAR, Release 2.1 or later	2 x Channelized OC3/STM1 ASAP	16

See Procedure 19-30 to create a multilink PPP bundle.

FR group bundles

FR group bundles are used to fragment lower priority DLCI frames to minimize jitter and delay on higher priority DLCI frames. The following general rules apply to FR group bundles.

- FR group bundles can only be created on channelized ASAP MDAs.
- FRF12 cannot be enabled on a SAP that is using an FR group bundle.
- DS0 channel groups must have all their timeslots selected and have their encapsulation type set to FR to be configured as bundle members.

Note — You can configure a maximum of 128 FR group bundles on an MDA.

See Procedure 19-32 to create a multilink PPP bundle.

19.6 Workflow to manage shelf objects

The following workflow describes the sequence of high-level tasks required to manage and configure shelf objects and shelf object children. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — Shelf objects and shelf object children can be accessed using the equipment navigation tree. See chapter 4 for more information about using the equipment navigation tree.

1 As required, perform the following procedures to configure shelf objects.

- **a** Configure the chassis mode of a device. See Procedure 19-1 for more information.
- **b** Configure dry-contact sensor monitoring. See Procedure 19-2 for more information.
- **c** Configure switch fabric multicast ingress replication rates. See Procedure 19-3 for more information.
- **d** Enable mixed mode on a 7450 ESS or 7750 SR device. See Procedure 19-4 for more information.
- **e** Configure timing synchronization. See Procedure 19-5 for more information.
- **f** Configure the IEEE 1588 clock on a 7705 SAR, version 4 or later. See Procedure 19-6 for more information.
- **g** Modify the IEEE 1588 PTP clock on the 7705 SAR. See Procedure 19-7 for more information.
- **h** Modify the IEEE 1588 PTP port on the 7705 SAR. See Procedure 19-8 for more information.
- **i** Configure auxiliary alarm definitions on the 7705 SAR. See Procedure 19-9 for more information.
- **j** Configure the IEEE 1588 PTP clock on a 7x50 SR device. See Procedure 19-10 for more information.
- **k** Configure the IEEE 1588 PTP peer on a 7x50 SR device. See Procedure 19-11 for more information.
- **l** Manage 9500 MPR running software. See Procedure 19-12 for more information.
- **m** Manage OmniSwitch running configuration. See Procedure 19-13 for more information.
- **n** Configure OmniSwitch health monitoring. See Procedure 19-14 for more information.

2 Assign a card type to a chassis slot. See Procedure 19-15 for more information.

3 As required, configure the card and card slot objects as follows:

   a Configure an egress WRED queue control on an IOM 3 or IMM forwarding plane. See Procedure 19-16 for more information.

   b Configure IMPM on a 2 x XP MDA IOM 3 or IMM forwarding plane. See Procedure 19-17 for more information.

   c Enable named pool mode. See Procedure 19-18 for more information.

   d Add or remove 9500 MPR card protection. See Procedures 19-19 and 19-20 for more information.

   e Configure OmniSwitch PoE ports. See Procedure 19-21 for more information.

   f Configure OmniSwitch stacks. See Procedure 19-22 for more information.

   g Configure an OmniSwitch CPU temperature threshold. See Procedure 19-23 for more information.

4 As required, configure daughter card objects as follows:

   a Configure an MDA. See Procedure 19-24 for more information.

   b Configure IMPM on an MDA. See Procedure 19-25 for more information.

   c View operational multicast channel properties on an MDA. See Procedure 19-26 for more information.

   d Configure a module card on the 7705 SAR-M/ME. See Procedure 19-27 for more information.

5 As required, create or modify bundle objects as follows:

   a multilink PPP bundle; see Procedures 19-28 and 19-29 for more information

   b IMA group bundle; see Procedures 19-30 and 19-31 for more information

   c FR group bundle; see Procedures 19-32 and 19-33 for more information

   d MLPPP bundle as a network interface on a channelized ASAP MDA; see Procedure 19-34 for more information

19.7 Shelf object configuration procedures

Use the following procedures to configure shelf objects using the navigation tree.

Procedure 19-1 To configure the chassis mode of a device

Perform this procedure to configure the chassis mode for the device. See chapter 16 for more information about chassis modes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the chassis mode and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative Mode

  If you downgrade the administrative chassis mode, the device must be rebooted to change the operational chassis mode.
- Force Mode

  Forcing a chassis mode change does not change the operational chassis mode unless there is a compatible card type equipped on the device. See chapter 16for more information about the minimum card type that must be installed for each chassis mode.

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 19-2 To configure dry contact sensors

Perform this procedure to configure dry contact sensors on a 7250 SAS-ESA or 7210 SAS-M 24F 2XFP ETR. See chapter 12 for information about dry contact sensors.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a dry contact sensor and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the External Alarms tab button. The Shelf Dry Contacts tab button is displayed.

5 Choose one of the dry contacts and click on the Properties button. The DryContact (Edit) form opens.

6 Configure the parameters:

- Name
- Description
- Monitored Status
- Polarity
- Alarm Severity
- Alarm Trigger Message
- Alarm Clear Message
- Control Status
- Control Type
- Connected To

7 Click on the OK button to close the DryContact (Edit) form.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 19-3 To configure switch fabric multicast ingress replication rates

Perform this procedure to configure the total multicast replication rates for primary and secondary ingress paths for each switch fabric multicast plane.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure switch fabric multicast ingress replication rates and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab button.

5 Configure the parameters:

- Primary Multicast Bandwidth (mbps)
- Secondary Multicast Bandwidth (mbps)
- Primary Multicast Bandwidth for Dual-SFM Mode (mbps)
- Secondary Multicast Bandwidth for Dual-SFM Mode (mbps)

6 Click on the OK button. The Shelf (Edit) form closes.

Procedure 19-4 To enable mixed mode on a 7450 ESS or 7750 SR device

Perform this procedure to enable mixed mode on a 7450 ESS or 7750 SR. Enabling mixed mode on a 7450 ESS-6v, 7450 ESS-7, or 7450 ESS-12, enables the support of features on the IOM3-XP and associated MDA-XPs or IMMs.

The 7750 SR-7 and 7750 SR-12, Release 9.0 R1 and later, support mixed mode. This support allows you to enable IPv6 on a 7750 SR in chassis mode A or B, without having to upgrade the entire chassis. Slots with network ports, and ports that require IPv6 support, can then be selectively upgraded for IOM3-XPs or IMMs.

Note — On the 7750 SR-7 and 7750 SR-12, Release 9.0 R5 and later, mixed mode cannot be enabled if an ISA TMS daughter card is configured on the node.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7450 ESS-6v, 7450 ESS-7, 7450 ESS-12, 7750 SR-7, or 7750 SR-12 device on which you want to enable mixed mode, and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Enable the Mixed Mode State on Chassis Enabled parameter.

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 19-5 To configure timing synchronization

Perform this procedure to configure timing synchronization. See chapter 16 for more information about timing synchronization.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure timing synchronization and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Timing tab button.

5 Configure the parameters, as required:

- Reference Input Mode (revertive)
- Reference Input Mode
- Reference Input Mode (revertive)
- Quality Level Reference
- First Timing Reference Input
- Second Timing Reference Input
- Third Timing Reference Input
- Fourth Timing Reference Input
- Type
- Interface Name
- Port or Channel Name
- Administrative State
- Quality Level Override
- First Timing Reference PTP Clock
- Second Timing Reference PTP Clock
- Role
- Wait to Restore Time (Min):
- Wait to Restore Time (Secs):
- Interface Type
- Input Administrative State
- Output Administrative State
- Output Line Length
- SSM
- Input Type
- Impedance Type
- Output Type
- Status
- Primary Reference Type
- Secondary Reference Type
- Sync In Port
- Sync Out Port

Note — The parameters that appear on the Shelf (Edit) form may vary, depending on the device type and version you are configuring.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button.The Shelf (Edit) form closes.

Procedure 19-6 To configure the IEEE 1588 PTP clock on a 7705 SAR-M/ME, or on a 7705 SAR, Release 4 or later

Perform this procedure to configure the IEEE 1588 PTP clock on a 7705 SAR-M/ME or a version 4.0 Release 3 or later 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 19-5 for more information about how to configure the 7705 SAR as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR device where you want to configure the IEEE 1588 PTP clock and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the IEEE PTP Clock tab button.

4 Click on the Create button. The IEEE 1588 PTP Clock (Create) form opens.

5 Configure the parameters:

- Clock ID
- Clock Type
- Clock Slave Only
- Admin State
- PTP Profile
- Dynamic Peers
- Clock Priority 1
- Clock Priority 2
- Domain

6 Click on the Select button beside the Clock MDA parameter and choose a source MDA for the PTP clock.

7 Click on the Select button beside the Interface Name parameter and choose a source interface for the PTP clock.

8 Click on the Apply button. A dialog box opens.

9 Click on the OK button.

10 As required, turn up PTP ports on the IEEE 1588 PTP clock.

i Choose a PTP port from the PTP Port panel and click on the Properties button. The IEEE 1588 PTP Port (Edit) form opens with the General tab displayed.

ii Configure the Admin State parameter.

iii Click on the OK button. The IEEE 1588 PTP Port (Edit) form closes.

11 Click on the OK button. A dialog box opens.

12 Click on the OK button. The IEEE 1588 PTP Clock (Create) form closes.

13 Click on the OK button to save the configuration and close the Network Element (Edit) form.

Procedure 19-7 To configure the IEEE 1588 PTP clock on the 7705 SAR

Perform this procedure to configure the IEEE 1588 PTP clock on a pre-version 4.0 Release 3 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 19-5 for more information about how to configure the 7705 SAR as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR device where you want to modify the IEEE 1588 PTP clock and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Timing tab button.

5 Click on the PTP Clock Properties button. The PTP Clock (Edit) form opens.

6 Configure the Domain parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The PTP Clock (Edit) form closes.

9 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 19-8 To modify the IEEE 1588 PTP port on the 7705 SAR

Perform this procedure to modify the IEEE 1588 PTP port on a 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 19-5 for more information about how to configure the 7705 SAR as a PTP client.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR device where you want to modify the IEEE 1588 PTP port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the Timing tab button.

5 Click on the PTP Port Properties button. The PTP Port (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Master 1 Address
- Master 2 Address
- Announce Receive Timeout
- Announce Interval
- Sync Interval

7 Click on the Recovered Clock History Master One tab button to view master 1 clock recovery statistics.

8 Click on the Recovered Clock History Master Two tab button to view master 2 clock recovery statistics.

9 Click on the OK button. The PTP Port (Edit) form closes.

10 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 19-9 To configure auxiliary alarm definitions on the 7705 SAR

Perform this procedure to configure auxiliary alarm definitions for the auxiliary alarms daughter card on a 7705 SAR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR device where you want to configure auxiliary alarm definitions and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

4 Click on the External Alarms tab button.

5 As required, configure auxiliary alarm digital inputs.

- **i** Click on the Auxiliary Alarm Digital Inputs tab button.
- **ii** Select a digital input from the list and click on the Properties button. The Auxiliary Alarm Digital (Edit) form opens with the General tab displayed.
- **iii** Configure the parameters:
  - Optional Name
  - Description
  - Administrative State
  - Detection (s)
  - Clearing (s)
  - State
- **iv** Click on the OK button. The Auxiliary Alarm Digital (Edit) form closes.
- **v** Repeat steps i to iv to configure more auxiliary alarm digital inputs, as required.

6 Click on the Auxiliary Alarm Definitions sub-tab button.

7 Click on the Create button. The Auxiliary Alarm Definition (Create) form opens.

8 Configure the following parameters:

- ID
- Auto-Assign ID
- Description
- Administrative State
- Severity

9 Click on the Inputs tab button and configure the following parameters:

- Trigger Rule
- Analog Threshold (mV)
- Operation
- Input 1 through Input 8 (as required)

10 Click on the Outputs tab button and configure the following parameters:

- Log Event
- Update Chassis Relays

11 Click on the OK button in the Auxiliary Alarm Definition (Create) form. A dialog box appears.

12 Click on the OK button.

13 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 19-10 To configure the IEEE 1588 PTP clock on a 7x50 SR7, SR12, ESS7, ESS12, or SR-c4, version 9 release 4 or later

Perform this procedure to configure the IEEE 1588 PTP clock on a version 9.0 Release 4 or later 7x50 SR7, SR12, ESS7, ESS12 or SR-c4 that is configured as an IEEE 1588 PTP client. See Procedure 19-5 for more information about how to configure the nodes as PTP clients.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the IEEE 1588 PTP clock and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the IEEE PTP Clock tab button.

4 Select an IEEE 1588 PTP Clock from the list and click on the Properties button. The IEEE 1588 PTP Clock (Edit) form opens.

5 Configure the parameters:

- Clock Type
- Admin State
- Clock Priority 1
- Clock Priority 2
- Domain
- Network Type

6 Click on the OK button. The IEEE 1588 PTP Clock (Edit) form closes.

7 Click on the OK button to save the configuration and close the Network Element (Edit) form.

Procedure 19-11 To configure the IEEE 1588 PTP peer on a 7x50 SR7, SR12, ESS7, ESS12, or SR-c4, version 9 release 4 or later

Perform this procedure to configure the IEEE 1588 PTP peer on a version 9.0 Release 4 or later 7x50 SR7, SR12, ESS7, ESS12 or SR-c4 that have the IEEE 1588 PTP clock configured. See Procedure 19-10 for more information about how to configure the IEEE 1588 PTP clock on the nodes.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the IEEE 1588 PTP clock and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the IEEE PTP Clock tab button.

4 Choose an entry in the list and click on the Properties button. The IEEE 1588 PTP Clock (Edit) form opens.

5 Click on the IEEE PTP Peers tab button.

6 Perform one of the following:

  a To create an IEEE 1588 PTP peer on a slave, go to step 7.

  b To modify an existing IEEE 1588 PTP peer on a slave, go to step 10.

7 Click on the Create... button. The IEEE 1588 PTP Peer (Create) form opens

8 Configure the parameters:

- Peer ID
- Peer IP Address
- Peer Priority
- Administrative State

9 Go to step 12.

10 Select an IEEE 1588 PTP peer from the list and click on the Properties button. The IEEE 1588 PTP Peer (Edit) form opens.

11 Configure the parameters:

- Peer Priority
- Administrative State

12 Click on the OK button. The IEEE 1588 PTP Peer (Create) form closes and a dialog box appears.

13 Click on the OK button. The IEEE 1588 PTP Clock (Edit) form reappears with the IEEE 1588 PTP Peer information displayed.

14 Click on the OK button. The Network Element (Edit) form reappears.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button to save the configuration and close the Network Element (Edit) form.

Procedure 19-12 To manage 9500 MPR running software

Perform this procedure to manage the software in the 9500 MPR committed and standby banks. You can upgrade or downgrade the running software version on a 9500 MPR. See chapter 23 for information about creating software upgrade policies and performing software upgrades.

Warning — A 9500 MPR may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility.

Caution — When you reboot a 9500 MPR that is in service it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the 9500 MPR device that you need to upgrade or downgrade and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Software Bank Details tab button. The committed and standby software information is displayed. The committed software is the software currently running on the 9500 MPR. The standby software is new software that was uploaded to the 9500 MPR or formerly committed software.

6 Verify that the operational state of the standby software is Enabled, by examining the Operational State column of the displayed list.

You can also examine the Software Version of the standby and committed software. If the software version of the standby software is newer than the committed software version, the 9500 MPR can be upgraded. If the standby software version is older than the committed software version, the 9500 MPR can be downgraded.

7 Choose the standby entry from the displayed list.

8 Click on the Properties button.

9 The MPRSoftwarePackage (Edit) form opens with the Software Bank Details tab displayed.

10 Configure the Activation parameter.

11 Click on the OK button. The MPRSoftwarePackage (Edit) form closes. The entry in the Activation column for the standby software should be the same as the option chosen in step 10.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. When the standby and committed software versions are different or the forced activation option is selected, the 9500 MPR reboots using the standby software. If the standby and committed software versions are the same and the activation option is chosen, the 9500 MPR does not reboot and the Shelf (Edit) form closes.

14 When the 9500 MPR reboots you can confirm that the 9500 MPR is running the software stored in the former standby bank. The former standby software is the committed software and the previous committed software is the standby software.

Procedure 19-13 To manage an OmniSwitch running configuration

Caution — When you reboot an OmniSwitch that is in service it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on a device and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Software Control Module tab button.

6 Configure the Command to Apply parameter.

  a If you specify Copy certified to working, configure the Active Timeout parameter.

  b If you specify Reload from working, configure the Delayed Activation Timer parameter.

7 Click on the OK button. The Shelf (Edit) form closes.

Procedure 19-14 To configure OmniSwitch Health Monitoring

The OmniSwitch Health Monitoring function monitors the consumable resources, such as bandwidth and CPU usage, of the switch. This function monitors the switch and at fixed intervals collects the current values for each resource being monitored. You can specify resource threshold limits and when a resource value falls above or below a threshold, traps are sent to the 5620 SAM.

Perform the following procedure to configure health monitoring on an OmniSwitch.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the OmniSwitch device that you need to configure OmniSwitch Health Monitoring and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Health Monitoring tab button.

6 Configure the following parameters:

- Rx Threshold (%)
- TxRx Threshold (%)
- Temperature Threshold Unit
- Temperature Threshold
- Memory Threshold (%)
- CPU Threshold (%)
- Sampling Interval (seconds)

7 Click on the Statistics tab button and search for Card Health Stats (Physical Equipment) or Device Health Stats (Physical Equipment) to view card statistics or chassis statistics respectively. Statistics can also be viewed from the card-level statistics tab.

8 Click on the Faults tab button to view alarm information.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Shelf (Edit) form closes.

19.8 Card and card slot object configuration procedures

Use the following procedures to configure card and card slot objects using the navigation tree.

Procedure 19-15 To assign a card type

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to assign a card type and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on an empty Card Slot object and choose Configure Card from the contextual menu. The Card Slot (Create) form opens.

5 Configure the parameters:

- Capability
- Assigned Card Type
- Shutdown IOM for Memory Parity Errors
- OLC State

Note — The correct chassis mode must be configured for the assigned card types. The chassis mode determines the behavior of the card and establishes the scaling limits and available features. See Procedure 19-1and 19-4 for more information.

6 Click on the OK button. The Card Slot (Create) form closes.

The card and slot appear in the navigation tree and in the equipment inventory list.

Procedure 19-16 To configure egress WRED queue control on an IOM 3 or IMM forwarding plane

Perform this procedure to configure the egress WRED queue control function on an IOM 3 or IMM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure egress WRED queue control on an IOM 3 or IMM forwarding plane and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Card Slot icon. The Card Slot (Create) form opens with the General tab displayed.

5 Click on the Forwarding Plane tab button.

6 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens.

7 Configure the Egress WRED Queue Control parameters:

- Administrative State
- Buffer Allocation Min (%)
- Buffer Allocation Max (%)
- Reserved CBS Min (%)
- Reserved CBS Max (%)

8 Click on the Select button in the Slope Policy panel. The Select Slope Policy - Forwarding Plane form opens.

9 Choose a policy in the list and click on the OK button. The Select Slope Policy - Forwarding Plane form closes, and the slope policy name is displayed in the Slope Policy panel.

10 Click on the OK button. The Forwarding Plane (Edit) form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 19-17 To configure IMPM on a 2 x XP MDA IOM 3 or IMM forwarding plane

Perform this procedure to configure IMPM on a 2 x XP MDA IOM 3 or an IMM.

Note — See Procedure 19-25 for information about configuring IMPM on an MDA that is not installed in a 2 x XP MDA IOM 3 or in an IMM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure IMPM and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Card Slot icon. The Card Slot (Create) form opens with the General tab displayed.

5 Click on the Forwarding Plane tab button.

6 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens.

7 Click on the Clear button to remove the selected policy. The Select button in the BW Policy panel is enabled.

8 Click on the Select button in the BW Policy panel. The Select BW Policy form opens.

9 Choose a policy in the list and click on the OK button. The Select BW Policy form closes, and the policy name is displayed in the BW Policy panel.

10 Configure the Admin State parameter.

11 Configure the following parameters:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm

12 Click on the OK button. The Forwarding Plane (Edit) form closes.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 19-18 To enable named pool mode

Perform this procedure to allow named pools to be created for an MDA. Set the pool mode parameter when you are configuring the card.

Caution — The Pool Mode parameter can be enabled and disabled at anytime, however changing the pool mode resets the IOM when MDAs are provisioned on the slot. If MDAs are not provisioned the IOM is not reset.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to enable named pool mode and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Click on a card slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the IO Card tab button.

6 Configure the Pool Mode parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 19-19 To add 9500 MPR card protection

The 9500 MPR supports card protection for all card types. EPS card protection for the CORE-ENH card in slot 1 is automatically configured by the system when an optional spare CORE-ENH card is provisioned into slot 2. Radio modem and 32 x DS1/E1 cards in slots 3, 5, and 7 can be protected by corresponding identical cards in slots 4, 6, and 8. Protection for cards in slots 3, 5, and 7 must be configured. The protected card is referred to as the main card and the protecting card is referred to as the spare card. Use the following procedure to configure optional card protection for radio modem and 32 x DS1/E1 cards.

Note 1 — All cross connections, flow-ids, and sync sources must be removed from the port under the spare card slot before protection can be enabled.

Note 2 — To configure protection type 1+1 FD on Radio, the Mode cannot be Adaptive Modulation.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR icon, right-click on the 9500 MPR object where you want to add card protection and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Click on the card slot object that you need to configure. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the Protection tab button.

6 Configure the following parameters on the main/spare card:

- Protection Type
- Restoration Criteria
- Commands

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Create) form closes.

9 Verify that the protection has been enabled. The status of the main card should be Active and the status of the spare card should be Standby.

Procedure 19-20 To remove 9500 MPR card protection

Note — If 1+1 HSB is configured as the protection type for a Radio card, the transmitter must be muted from the NEtO to remove the protection.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand the 9500 MPR icon, right-click on the 9500 MPR object where you want to remove card protection and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. On the Network Element (Edit) form navigation tree, expand the Shelf icon.
4. Click on the card slot object that you need to configure. The Card Slot (Edit) form opens with the General tab displayed.
5. Click on the Protection tab button.
6. Set the Protection Type parameter to No Protection.
7. Click on the OK button. A dialog box appears.
8. Click on the Yes button. The Card Slot (Create) form closes.
9. Verify that the protection has been removed from the previously main and spare cards.

Procedure 19-21 To configure OmniSwitch PoE Ports

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand the OmniSwitch icon, right-click on an OmniSwitch device and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
3. On the Network Element (Edit) form navigation tree, expand the Shelf icon.
4. Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.
5. Click on the PoE tab button.
6. Configure the parameters:
   - Slot Priority
   - Power State
   - Port Maximum Power (MilliWatts)
   - Maximum Power (Watts)
   - Enable Priority Disconnect
   - Enable Power Capacitor Detection
   - Combo Port

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 19-22 To configure OmniSwitch stacks

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch icon, right-click on an OmniSwitch device and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the Stack Configuration tab button.

6 Configure the parameters, as applicable to a given OmniSwitch NE:

- Saved Slot NI Number
- Command Action
- Stacking Action
- Administrative
- Operational

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 19-23 To configure an OmniSwitch CPU temperature threshold

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch icon, right-click on an OmniSwitch device and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Click on a slot object. The Card Slot (Edit) form opens with the General tab displayed.

5 Click on the Hardware Environment tab button.

6 Configure the Temperature Threshold (Celsius) parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Card Slot (Edit) form closes.

19.9 Daughter card slot object configuration procedures

Use the following procedures to configure daughter card slot objects using the navigation tree.

Procedure 19-24 To configure an MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an MDA and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon and the Card Slot icon.

4 Perform one of the following.

a To add a daughter card to an empty daughter card slot, right-click on the daughter card slot and choose Configure Daughter Card from the contextual menu. The Daughter Card Slot (Create) form opens.

b To modify an existing daughter card, click on the daughter card slot. The Daughter Card Slot (Edit) form opens.

Note — If daughter card in your configuration is managed by 5620 SAM but becomes no longer supported by 5620 SAM (for instance, an obsoleted MDA), it will be displayed under the equipment tree as type Unspecified. To delete such a card from 5620 SAM, you must remove the MDA from the device. Once a card is removed from the device, it is also automatically deleted from 5620 SAM.

5 Configure the parameters:

- Assigned Daughter Card Type
- In MDA Carrier Module Slot
- OLC State
- ATM Mode

Note 1 — The Assigned Daughter Card Type and In MDA Carrier Module Slot parameters are configurable only during daughter-card creation.

Note 2 — The ATM Mode parameter can only be configured on an MDA card of type 4 x ATM OC3/OC12, 4 x ATM OC3 STM1, or 16 port ATM OC3 STM1 on 7x50 cards (including the Portugal and Alberta cards but excluding SR-C12 and SR-c4 chassis) beneath an IOM 3 card.

Note 3 — The ATM Mode parameter must be set to a value of max16k-vc for PPPoA and PPPoEoA to be supported.

6 If you are creating a daughter card on a 7710 SR, perform the following steps.

i Click on the MDA Carrier Module tab button.

ii Configure the Assigned MCM Card Type parameter.

7 Click on the Apply button.

8 Click on the Daughter Card tab button.

9 Configure the parameters:

- Administrative State
- MDA Mode
- Synchronous Ethernet

Note 1 — The MDA Mode parameter can only be configured on 16 x Channelized DS1/E1 ASAP v2, 32 x Channelized DS1/E1 ASAP v2, 4 x Channelized DS1/E1 ASAP, or XMDA 1p x 10GigE / 10p x 1GigE SFP.

Note 2 — Before you configure the MDA Mode parameter, you must shut down all of the ports and remove all of the subchannels and bundles from the MDA.

10 Configure the following parameters in the Voice panel, if required:

- Companding Law
- Signalling Type

11 Perform the following steps to configure named buffer pools, if required.

Note — You must enable pool mode on the parent I/O card to enable named buffer pool support. See Procedure 19-18 for more information.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. The Select Ingress Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Ingress Pool Policy form closes, and the policy name is displayed in the Ingress Pool Policy panel.

iii If you are configuring an HSMDA daughter card, go to step 12.

Note — HSMDA daughter cards support only ingress named buffer pool policies, and not egress named buffer pool policies.

iv Click on the Select button beside the Name parameter in the Egress Pool Policy panel. The Select Egress Pool Policy form opens.

v Choose a policy in the list and click on the OK button. The Select Egress Pool Policy form closes, and the policy name is displayed in the Egress Pool Policy panel.

12 Perform the following steps to configure HSMDA pool policies, if required.

Note — You must enable pool mode on the parent I/O card to enable HSMDA pool support. See Procedure 19-18 for more information.

i Click on the Select button in the Egress HSMDA Pool Policy panel. The Select Egress HSMDA Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Egress HSMDA Pool Policy form closes, and the policy is displayed in the Egress HSMDA Pool Policy panel.

13 Configure the following parameters in the HSMDA Aggregate Queue Burst panel, if required:

- Threshold Low Burst Multiplier
- Threshold High Burst Increase

14 Perform the following steps to add a fabric profile, if required.

i Click on the Select button in the Network Ingress Fabric Profile panel. The Select Fabric Profile form opens.

ii Choose a profile in the list and click on the OK button. The Select Network Ingress Fabric Profile form closes, and the profile name is displayed in the Network Ingress Fabric Profile panel.

iii Click on the Select button in the Access Ingress Fabric Profile panel. The Select Fabric Profile form opens.

iv Choose a profile in the list and click on the OK button. The Select Access Ingress Fabric Profile form closes, and the profile name is displayed in the Access Ingress Fabric Profile panel.

15 Perform steps 2 to 5 of Procedure 19-25 to configure IMPM on the daughter card, if required.

16 If you configured named buffer pools in step 11, perform the following steps to configure the associated Q1 pools. Otherwise, go to step 17.

Note — You cannot use this step to configure 7710 SR QoS policies.

i Click on the QoS Pool tab button.

ii Choose a pool in the list and click on the Properties button. The QoS Pool (Edit) form opens.

iii Configure the parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

iv Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

v Choose a policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes, and the slope policy name is displayed in the Slope Policy panel.

17 Perform the following steps to configure ATM, if required.

i Click on the ATM tab button.

ii Select an ATM configuration from the list and click on the Properties button. The ATM Configuration (Edit) form opens.

iii Click on the VP Shaping tab button.

iv Click on the Create button. The ATM VP Shaper (Create) form opens.

v Configure the VP ID parameter.

vi Click on the Select button in the ATM QoS Policy panel. The Select ATM QoS Policy - ATM VP Shaper form opens.

vii Select an ATM QoS Policy from the list and click on the Properties button. The ATM QoS Policy (Edit) form opens.

- **viii** Click on the QoS tab button.
- **ix** Configure the VP Shaping Weight parameter.
- **x** Click on the OK button. A dialog box appears.
- **xi** Click on the Yes button. The ATM QoS Policy (Edit) form closes.
- **xii** Click on the OK button. The Select ATM QoS Policy - ATM VP Shaper form closes.
- **xiii** Click on the OK button. A dialog box appears.
- **xiv** Click on the OK button. The ATM VP Shaper (Create) form closes.
- **xv** Repeat steps iv to xiv to create additional ATM VP shapers, if required.
- **xvi** Click on the OK button. A dialog box appears.
- **xvii** Click on the Yes button. The ATM Configuration (Edit) form closes.

18 Click on the OK button. A dialog box appears.

If you are adding a new daughter card, the daughter card and the contained ports are displayed in the navigation tree.

19 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 19-25 To configure IMPM on an MDA

Perform this procedure to configure IMPM on an MDA that is not installed in a 2 x XP MDA IOM 3 or an IMM.

Note — See Procedure 19-17 for information about configuring IMPM on a 2 x XP MDA IOM 3 or IMM.

1 Perform steps 1 to 8 of Procedure 19-24.

2 Configure the following parameters in the Daughter Card Details panel:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm

3 Click on the Select button in the BW policy panel to choose a multicast bandwidth policy. The Select BW Policy form opens.

4 Choose a policy in the list and click on the OK button. The Select BW Policy form closes and the policy name is displayed in the BW Policy panel.

Note — The multicast bandwidth policy named “default” cannot be modified or deleted.

5 Configure the following parameters in the Multicast Path Management panel:

- Admin State
- Primary Path Limit (mbps)
- Secondary Path Limit (mbps)
- Ancillary Path Limit (mbps)

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 19-26 To view operational multicast channel properties on an MDA

Perform this procedure to view specific information about an operational multicast channel on an MDA that is configured to use an Ingress Multicast Bandwidth policy.

Note — You can also view operational multicast channel information in the following locations:

- the Mcast Path Mgmt tab on the properties form of a VPLS or VPRN service site
- the Mcast Path Mgmt Channels tab on the properties form of a routing instance.

Each properties form contains information about the ingress MDA of each operational channel.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to view operational multicast channel properties on an MDA and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Card Slot icon. The Card Slot (Create) form opens with the General tab displayed.

5 Click on the daughter card slot object. The Daughter Card Slot (Edit) form opens with the General tab displayed.

6 Click on the Mcast Path Mgmt Channels tab button.

7 Click on the Search button. A list of operational channels is displayed.

8 View the information, which includes the service site or routing instance associated with the channel, and the following properties:

Note — Channel information is displayed only when the MDA receives multicast traffic for a previously configured multicast group.

- Group Address—the operational channel multicast group address
- Source Address—the operational channel multicast source address
- Bandwidth—the operational bandwidth of the channel
- Administrative Bandwidth—the administrative bandwidth of the channel
- Last Highest Bandwidth—the value of the multicast bandwidth that is currently allocated to the channel forwarding path on the MDA. This value is calculated based on periodic statistics polls and represents the highest recorded bandwidth value since the most recent restart of the bandwidth update timer for the channel.
- Second Highest Bandwidth—the second-highest recorded bandwidth value for the channel since the most recent restart of the bandwidth update timer. The value is calculated based on periodic statistics polls and is reset to zero every time the bandwidth update timer for the channel is restarted.
- BW Update Timer expiration—the time that remains before the bandwidth update timer for the channel expires
- Current Path—the path that the channel traffic uses to reach the switching fabric; the path value is primary, secondary, or ancillary
- Explicit Path—indicates whether the current path is explicitly specified by a Multicast Info Policy
- Preference Level—the preference level of the channel
- Black-Hole—whether the channel is in the Black-Hole state
- Black-Hole Rate—specifies the bandwidth rate, in kb/s, at which the channel enters the Black-Hole state

9 Close the Daughter Card Slot (Edit) form.

Procedure 19-27 To configure a module card on the 7705 SAR-M/ME

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 7705 SAR-M/ME device on which you need to configure an MDA and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon and the Card Slot icon.

4 Right-click on the third Daughter Card Slot icon and choose Configure Daughter Card from the contextual menu. The Daughter Card Slot (Create) form opens with the General tab displayed.

Note — Only the third daughter card slot can be configured with module cards. The other two slots are configured with integrated cards that cannot be removed.

5 Configure the Assigned Daughter Card Type parameter.

6 Click on the Apply button. The Daughter Card Slot form refreshes.

7 Click on the Daughter Card tab button.

8 Configure the parameters:

- Administrative State
- Fabric Stats

9 Add a fabric profile, if required:

i Click on the Select button in the Network Ingress Fabric Profile panel. The Select Fabric Profile form opens.

ii Choose a profile and click on the OK button. The Select Network Ingress Fabric Profile form closes and the profile name is displayed in the Network Ingress Fabric Profile panel.

iii Click on the Select button in the Access Ingress Fabric Profile panel. The Select Fabric Profile form opens.

iv Choose a profile and click on the OK button. The Select Access Ingress Fabric Profile form closes and the profile name is displayed in the Access Ingress Fabric Profile panel.

If you are configuring a 1 Colour Optical Add/Drop Mux card, go to step 25.

10 Click on the Ports tab button.

11 Choose a port and click on the Properties button. The Physical Port (Edit) form opens with the General tab displayed.

Note — The first port on the DCM includes four SHDSL lines. The second port includes two XDSL lines.

12 Configure the parameters:

- Description
- Configured MAC
- Mode
- Encap Type
- Speed
- MTU (bytes)
- DDM Event Suppression
- OLC State

13 Click on the States tab button.

14 Configure the Administrative State parameter. If you are configuring a DCM or DSL module, go to step 17.

15 Click on the GPON tab button.

16 Configure the parameters and go to step 22:

- Subscriber Location ID (SLID)
- Dot1 Q Ethertype
- CFM LoopBack Mode
- Egress Rate (Kbps)
- Type
- Time (seconds)

17 Click on the DSL tab button.

18 Configure the parameters:

- Dot1 Q Ethertype
- CFM LoopBack Mode
- Adsl2Plus
- Egress Rate (Kbps)
- Type
- Time (seconds)
- Synchronous status messages
- SSM Code-Type

19 Configure XDSL or SHDSL lines, if required.

i Click on the XDSL or SHDSL tab button, as appropriate.

ii Choose an XDSL or SHDSL line and click on the Properties button. The XDSL Line (Edit) or SHDSL Line (Edit) form opens with the General tab displayed.

iii Configure the Administrative State parameter.

iv Click on the OK button. The XDSL Line (Edit) or SHDSL Line (Edit) form closes.

v Repeat steps i to iv to configure more lines, if required.

20 Click on the Ethernet tab button.

21 Perform steps 7 to 11 of Procedure 38-42.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The Physical Port (Edit) form closes.

24 If you are configuring a DCM, repeat steps 11 to 23 to configure the second port.

25 Close the Daughter Card Slot (Edit) form.

19.10 Bundle configuration procedures

Use the following procedures to manage bundles using the navigation tree.

Procedure 19-28 To create a multilink PPP bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to a multilink PPP bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

5 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

6 Click on the Next button. The Configure Bundle Parameters form opens.

7 Set the Bundle Type parameter to PPP.

Note 1 — To create an IMA group bundle, perform Procedure 19-30.

Note 2 — To create an FR group bundle, perform Procedure 19-32

8 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

9 Click on the Next button. The Configure Bundle Members form opens.

10 Click on the Add button to add DS0 channel groups to the bundle.

The Add Bundle Member series of configuration steps appears.

11 Configure the Show Only Compatible Channels parameter.

12 Click on the Next button.

The Select Channels form opens.

13 Select compatible channels from the list to construct the bundle.

Add channels to a bundle as follows:

- Choose up to eight channel groups from the list of channels.

Note 1 — If there are no compatible channels to choose from and you have decided that you want to edit some of the existing channels that are not compatible to be compatible, click on the Back button and disable the Show Only Compatible Channels parameter. Click on the Next button. Choose channels to edit from the list and click on the Properties button.

Note 2 — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

14 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form re-opens.

15 Click on the Finish button.

16 Click on the Close button. The Create Multilink Bundle form closes.

17 Use the Properties contextual menu to view information about the created bundle, or modify bundle parameters.

- The General tab displays the Bundle ID, CLI name, MTU (bytes), Mode, and Encap Type parameters.
- The MultiLink Bundle tab displays the bundle type, bundle parameters, and link information.
- The L2 Interfaces and L3 Interfaces tab lists the interfaces that the bundle is assigned to.
- The States tab displays information about the operational and administrative state of the bundle.
- The Bundle Members tab lists the bundle members. From this form you can view member information and add or remove members from the bundle.
- Statistics and fault information is available from the appropriate tabs.

Procedure 19-29 To modify a multilink PPP bundle

Perform the following procedure to edit multilink PPP bundle parameters, add group members, and configure MC MLPPP to allow multiple classes of services to be transmitted over the bundle.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify a multilink PPP bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Bundles icon and click on a multilink bundle object. The Multilink Bundle (Edit) form for the PPP bundle opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Multilink Bundle tab button.

7 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

8 Click on the States tab.

9 Configure the Administrative State parameter, if required.

10 Configure the MLPPP bundle for multiclass service transmission. Perform the following steps.

Note — Consider the following when you configure MC MLPPP.

- MC MLPPP is supported only on channelized ASAP MDAs in the 7705 SAR, Release 2.0 or later, 7710 SR, and 7750 SR.
- You must configure MC MLPPP before you add bundle members to the multilink bundle.
- MC MLPPP is not supported when the port is configured as network mode.
- MC MLPPP is not supported when LFI is enabled.

i Click on the MLPPP tab button.

ii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number
- Stateless Aps Switchover

Note — The Magic Number parameter is configurable only on 7710 SR and 7750 SR channelized ASAP MDAs.

iii Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose an MLPPP ingress or egress QoS profile. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.

Note — You can only apply QoS profiles to an MLPPP bundle if the Class Count parameter is set to 4.

iv Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button.

11 To add members to the multilink bundle, perform the following steps.

i Click on the Bundle Members tab button.

ii Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform steps 11 to 13 of Procedure 19-28.

iv Click on the Finish button. The Add Bundle Member series of configuration steps closes.

Note — You can also add bundle members to the multilink bundle using the contextual menu in the navigation tree.

12 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

13 Click on the Service Access Points tab button to view SAP information.

14 Click on the Statistics tab button to view statistical information.

15 Click on the Faults tab button to view information about alarms.

16 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 19-30 To create an IMA group bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create an IMA group bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

5 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

6 Click on the Next button. The Configure Bundle Parameters form opens.

7 Set the Bundle Type parameter to IMA.

Note 1 — To create a PPP group bundle, perform Procedure 19-28.

Note 2 — To create an FR group bundle, perform Procedure 19-32

8 Configure the parameters:

- Bundle Type
- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

9 Click on the Next button. The Configure Bundle Members form opens.

10 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 11.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Add button. The Add Bundle Member series of configuration steps appears.

ii Click on the Next button. The Select Channels form opens.

iii Choose up to 8 channel groups from the list of channels to construct the bundle.

Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

11 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

12 Close the Create Multilink Bundle form.

Procedure 19-31 To modify an IMA group bundle

Perform the following procedure to edit IMA group bundle parameters, add group members, and specify a test member for IMA group bundle connectivity testing.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify an IMA group bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Bundles icon and click on an IMA group bundle object. The Multilink Bundle (Edit) form for the IMA group bundle opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Multilink Bundle tab button.

7 Configure the parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

8 To specify the IMA member that is used to test link connectivity in the IMA group bundle, perform the following steps.

i Click on the Select button beside the Test Member parameter. The Select Interface - Multilink Bundle form opens.

ii Choose an interface from the list.

iii Click on the OK button. The Select Interface - Multilink Bundle form closes and the Multilink Bundle (Edit) form refreshes with the test member information.

9 Click on the More Actions button and choose Test Pattern Start to run the test. You can click on the More Actions button and choose Test Pattern Stop at any time to stop the test. The Multilink Bundle (Edit) form refreshes with the link connectivity information.

10 Click on the States tab.

11 Configure the Administrative State parameter, if required.

12 To add members to the IMA group bundle, perform the following steps.

- **i** Click on the Bundle Members tab button.
- **ii** Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.
- **iii** Perform step 10 b of Procedure 19-30.

Note — You can also add bundle members to the IMA group bundle using the contextual menu in the navigation tree.

13 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

14 Click on the Service Access Points tab button to view SAP information.

15 Click on the Statistics tab button to view statistical information.

16 Click on the Faults tab button to view information about alarms.

17 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 19-32 To create an FR group bundle

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create an FR group bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the Bundles object and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

5 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

6 Click on the Next button. The Configure Bundle Parameters form opens.

7 Set the Bundle Type parameter to FR.

Note 1 — To create a PPP group bundle, perform Procedure 19-28.

Note 2 — To create an IMA group bundle, perform Procedure 19-30

8 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

9 Click on the Next button. The Configure Bundle Members form opens.

10 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 11.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Add button. The Add Bundle Member series of configuration steps appears.

ii Click on the Next button. The Select Channels form opens.

iii Choose up to 8 channel groups from the list of channels to construct the bundle.

Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

11 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

12 Close the Create Multilink Bundle form.

Procedure 19-33 To modify an FR group bundle

Perform the following procedure to edit FR group bundle parameters, add group members, and specify a test member for FR group bundle connectivity testing.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify an FR group bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Bundles icon and click on an FR group bundle object. The Multilink Bundle (Edit) form for the FR group bundle opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Multilink Bundle tab button.

7 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

8 Click on the MLFR tab button.

9 Configure the parameters:

- Hello Timer
- Ack Timer
- Hello Retry Count

10 Click on the Select button beside the MCFR Ingress Qos Profile parameter. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form opens.

11 Choose a profile from the list and click on the OK button. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Ingress QoS Profile information.

12 Click on the Select button beside the MCFR Egress Qos Profile parameter. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form opens.

13 Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Egress QoS Profile information.

14 Click on the States tab.

15 Configure the Administrative State parameter, if required.

16 To add members to the FR group bundle, perform the following steps.

i Click on the Bundle Members tab button.

ii Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform step 10 b of Procedure 19-30.

Note — You can also add bundle members to the FR group bundle using the contextual menu in the navigation tree.

17 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

18 Click on the Service Access Points tab button to view SAP information.

19 Click on the Statistics tab button to view statistical information.

20 Click on the Faults tab button to view information about alarms.

21 Configure the FR interface, if required. Perform the following steps:

i Click on the More Actions button and choose Edit FR. The FR Interface form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Error Threshold
- Monitored Events
- Polling Interval
- Full Enquiry Interval

22 Click on the OK button. The FR Interface form closes.

23 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 19-34 To configure an MLPPP bundle as a network interface on a channelized ASAP MDA

1 Perform Procedure 19-28 to create a MLPPP bundle on a channelized ASAP MDA.

Note — Consider the following when configuring an MLPPP as a network interface.

- LFI is not supported on MLPPP network interfaces.
- MC MLPPP is not supported on MLPPP network interfaces.
- IPv6 network interfaces are not supported.
- Up to 8 network interface members can be added to a bundle.

2 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

3 Right-click on the device where you want to configure an MLPPP bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand the Bundles icon and click on the bundle created in step 1. The Multilink Bundle (Edit) form opens with the General tab displayed.

6 Click on the Bundle Members tab button.

7 Click on the Search button and choose a bundle member from the list. Click on the Properties button. The Bundle Member (Edit) form opens.

8 Click on the Port tab button.

9 Click on the Properties button beside the port name. The DS0 Channel Group (Edit) form opens with the General tab displayed.

10 Set the Mode parameter to Network.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The DS0 Channel Group (Edit) form closes.

13 Close the Bundle Member (Edit) form.

14 The Multilink Bundle (Edit) form refreshes with new tabs.

15 Click on the Network Interfaces tab button.

16 Click on the Create button. The Create Network Interface - Routing Instance form opens.

17 Perform steps 4 to 42 of Procedure 30-7 to create a network interface on the DS0 channel.

The port in step 6 of Procedure 30-7 is set to the DS0 channel by default. Go to step 11 of Procedure 30-7.

18 The L3 interface appears on the Network Interfaces tab. Close the Multilink Bundle (Edit) form.

20 — Port and channel object configuration

20.1 Port and channel object configuration overview

Port objects are children of daughter card slot objects. They appear below the daughter card slot after the daughter card is configured. Channel objects are children of port objects. They appear on the navigation tree below the port object after the channel is configured.

Properties forms for port objects and channel objects are accessed using the 5620 SAM navigation tree.

This chapter contains the procedures to configure devices using the navigation tree. See chapter 4 for more information about using the navigation tree.

20.2 Working with port and channel objects

The types of ports available depend on the daughter cards that are configured in the chassis. For some OmniSwitch devices, the ports that are available depend on the chassis type, for others the type of card that is configured for the card slot. Ethernet ports cannot be channelized. SONET/SDH and TDM ports can be channelized. The following types of ports are supported:

- Fast Ethernet (10/100/1000 Base-T)
- Gigabit Ethernet (1000Base-T)
- 10 Gigabit Ethernet (10000Base-T)
- 10 Gigabit Ethernet (10GBase-T)
- 40 Gigabit Ethernet (10GBase-T)
- Ethernet combo
- PoE
- OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, and OC-192/STM-64 SONET/SDH
- channelized OC-3 and DS3/E3
- channelized ASAP OC-3/STM-1, OC-12/STM-4, DS1/E1, and DS3/E3

The port syntax for most devices that support daughter cards is card slot/daughtercard/port. For example, Port 1/1/1 represents port 1 of daughter card 1 in slot 1. The port syntax for the OmniSwitch is card slot/port. In every case, ports are created automatically when the daughter card is created. You must select one port object at a time and configure the properties of the port for the service that you need the port to provide. The properties vary depending on whether the port type is one of the Ethernet ports, SONET/SDH ports, or TDM ports. Channel objects are created on SONET/SDH or TDM ports for any type of channelization on the port whether it is a clear channel application or a sub-channel application.

Use the properties forms available from the contextual menus in the navigation tree to configure port and channel parameters. You can configure the port mode as network, access, or hybrid.

- Network ports pass network-level traffic.
- Access ports are customer-facing and pass service-level traffic.
- Hybrid ports can pass network-level and access-level traffic.

Note 1 — By default, a port is in Network mode.

Note 2 — See Procedure 20-2 to change the port mode.

Clear channel ports (OC-192/OC-48c/OC-12c/OC-3c) are either network or access ports. Channelized ports (CHOC-12/CHOC-3c/ DS3/E3) are always in access mode, however, the ASAP CHOC-3 supports both access and network modes. The ASAP DS1/E1 ports support:

- access mode for ATM/IMA and TDM
- network mode for PPP/MLPPP

Network ports are used in the service provider transport or infrastructure network, such as an IP/MPLS-enabled backbone network or uplink ports for rings using L2 Ethernet switches, such as the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco. A port that is in network mode can be assigned an IP address and host an L3 interface that can perform IP routing functions.

Note — The number of network interfaces that you can configure on one port is increased considerably in Release 8.0 and later NEs to support hybrid port applications. See the appropriate device documentation for specific interface configuration limits.

Access ports are associated with a SAP, a subscriber, and a service to provide connectivity. Access ports and channels are configured with encapsulation values to differentiate the service on the port or channel. When a port is access mode, one or more services can be configured on the port. A channelized port that is to act as an endpoint must be in access mode. You can convert access ports to hybrid ports and migrate any existing SAPs. See Procedure 20-3 for more information.

Hybrid ports are ports that can host SAPs and network interfaces simultaneously. This enables a customer to use one uplink port for enterprise and end-user traffic. A hybrid port preserves the existing network and access port functionality, and uses the same QoS, scheduler, and port scheduler resources as other ports, but requires the configuration of weight values that allocate buffer percentages to the access and network traffic on the port.

The 5620 SAM supports hybrid mode configuration for Ethernet ports on Release 8.0 or later of the 7450 ESS, 7750 SR-7, and 7750 SR-12 in any chassis mode.

Note — The 7450 ESS-1 and 7750 SR-1 do not support hybrid port mode.

You can configure a hybrid port on an Ethernet MDA in an IOM-3XP, or on a CMA in an IOM-XP. The 7750 SR supports hybrid port configuration on an IMM in addition to an IOM-3XP.

Note — Hybrid port configuration is not supported on an HSMDA or a VSM MDA.

A hybrid port supports dot1q and Q in Q encapsulation, but does not support null encapsulation, in order to accommodate single-SAP operation. The available VLAN tags are shared among the VLAN SAPs and VLAN network IP interfaces. When you create a SAP or L3 interface on a hybrid port, the outer VLAN tag must not be in use by another SAP or L3 interface on the port.

By default, the MTU of a hybrid port is set to the larger of the network and access MTUs to accommodate the creation of L3 interfaces and SAPs.

Note 1 — A hybrid port can participate in a single-chassis LAG.

Note 2 — A hybrid port cannot participate in an MC-LAG or MC ring.

See the appropriate device documentation for more information about hybrid ports.

When working with a TDM port, you must specify the Line Buildout as either short or long. That is, for a DS3 port the Line Buildout parameter must be configured. If the TDM port is in the context of a SONET STS-1 sub-channel, for example, the DS3 channel is built on the STS-1 channel of a SONET port, the line buildout parameter is not required.

At the connection termination points, you are required to configure the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel.

Policies can be added or deleted as required using the manage policy forms.

You can associate policies to ingress and egress access and network ports. Buffer policies are used to create and edit QoS buffer pool resources on network ports, access ports, and access channels. Egress network ports, access ports, and access channels have a dedicated buffer pool for queuing. The traffic is handled by a single buffer pool, one at the ingress, and one at the egress.

You can configure the amount of egress buffer space to be allocated to the port or channel. By default, all egress buffers are allocated fairly among the egress ports and channels based on their relative egress bandwidth.

The egress buffers for egress network ports and channels are put into per-port or per-channel egress buffer pools and are used by the egress network forwarding class queues on that port or channel. The ingress buffers allocated to network ports and channels are summed into a single pool and are used by the ingress network forwarding class queues (defined by the network ingress buffer policy).

The egress and ingress buffers allocated to access ports and channels are put into an egress buffer pool and ingress buffer pool for the port or channel. The access buffer pools are used by egress and ingress service queues created by the SAP-egress and SAP-ingress policies in use by services on the port or channel.

Changing the size of an egress buffer pool should be carefully planned. By default, there are no free buffers to increase the size of a pool. In order to increase a pool on one port or channel, the same amount of buffers must be freed from other egress buffer pools on the same daughter card.

Digital diagnostics monitoring

The 5620 SAM displays the following digital diagnostics monitoring data and alarm and warning information for ports on SFPs and XFPs optical modular transceivers:

- temperature
- supply voltage (SFP)
- TX bias
- TX output power
- RX received optical power
- external calibration

The transceiver is programmed with warning and alarm thresholds for low and high conditions that can generate system events. The thresholds for SFPs and XFPs are programmed by the transceiver manufacturer. The 5620 SAM raises an alarm when these thresholds are exceeded.

You can view digital diagnostics monitoring information from the DDM tab on the property form of supported ports. The External Calibration tab is available if the ports on SFPs and XFPs optical modular transceivers support the external calibration functionality.

Tagged and untagged VLAN ports

Consider the following when you create VLANs on CLE devices, such as 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices.

- You must configure the 7250 SAS and Telco uplink ports in network mode, to allow a physical connection, which is called the uplink, to the network device that feeds the traffic ring, such as a 7450 ESS.
- The 5620 SAM supports tagged and untagged ports as VLAN access ports.

Table 20-1 describes the behavior when ingress tagged or untagged traffic enters and then exits a VLAN.

Table 20-1 Tagged and untagged traffic behavior

<table>
<tr><th>Ingress traffic configuration</th><th>Ingress VLAN port configuration</th><th>Action</th><th>Egress VLAN port configuration and action</th></tr>
<tr><td rowspan="4">Untagged</td><td rowspan="2">Untagged</td><td rowspan="4">The VLAN allows the traffic and passes it based on the default VLAN ID.
The MAC address of the destination is learned.</td><td>If the egress VLAN port is untagged, the traffic remains untagged.</td></tr>
<tr><td>If the egress VLAN port is tagged, a tag is added to the traffic.</td></tr>
<tr><td rowspan="2">Tagged</td><td>If the egress VLAN port is untagged, the traffic remains untagged.</td></tr>
<tr><td>If the egress VLAN port is tagged, a tag is added to the traffic.</td></tr>
<tr><td rowspan="4">Tagged</td><td rowspan="2">Untagged</td><td rowspan="2">The VLAN allows the traffic if the tag matches the default VLAN ID.
The MAC address of the destination is learned.
If the tag does not match the default VLAN ID, the traffic is dropped.</td><td>If the egress VLAN port is untagged, the tag of the traffic is removed.</td></tr>
<tr><td>If the egress VLAN port is tagged, the traffic remains tagged.</td></tr>
<tr><td rowspan="2">Tagged</td><td rowspan="2">The VLAN allows the traffic:
• if the tag matches the default VLAN ID
• if the tag matches another VLAN ID
The MAC address of the destination is learned.
If the tag does not meet either condition, the traffic is dropped.</td><td>If the egress VLAN port is untagged, the tag of the traffic is removed.</td></tr>
<tr><td>If the egress VLAN port is tagged, the traffic remains tagged.</td></tr>
</table>

Figures 20-1 and 20-2 show how tagged and untagged traffic is handled on the devices, based on the VLAN ID.

Figure 20-1 Untagged traffic and VLANs

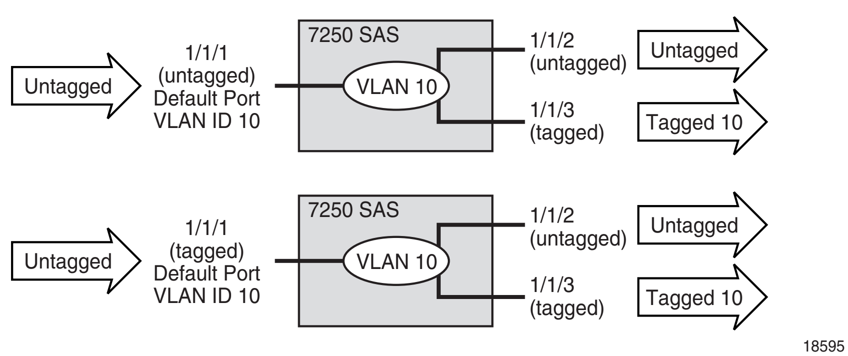
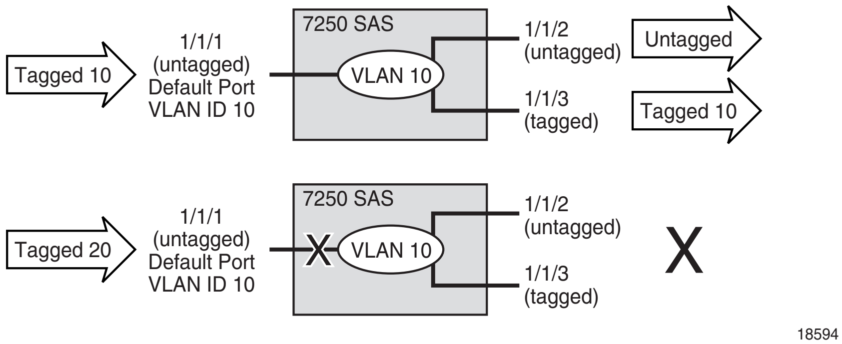


Figure 20-2 Tagged traffic and VLANs



Connection termination points for services and interfaces

Connection termination points are objects that represent terminating endpoints for a service, for example the endpoint of a VLL service. Connection termination points can be Layer 2 or Layer 3 interfaces, depending on the type of service being created. At the connection termination points you must configure the mode as Access or Network, the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel. The following objects can be used for connection termination points:

- STS-3 to STS-192 clear channels
- DS3 clear channel
- DS0 groups
- ports
- bundle

STS-3 to STS-192 clear channel

STS-3 to STS-192 clear channel SONET/SDH ports can be used to create SAPs or IP interfaces with one clear channel on each port that operates at the rate of the parent object. Clear channel SONET applications can be performed on any OC-*n* card. SONET channel termination for 1 x 10-Gig MDAs are not supported. See “SONET clear channel applications” in this section for more information.

DS3 clear channel

A DS3 clear channel can be a connection termination point when it is explicitly configured as unchannelized, that is, when the Configuration Type is set to None, which is the default setting for a DS3. DS3 clear channel connections cannot be channelized to a lower level than the one full DS3 channel. See “TDM channelization and clear channel applications” in this section for more information.

DS0 channel groups

A TDM channel group connects a group of DS0s by allocating a specific number of spans or interfaces and channels to a group of channels. The DS0 channel group defines the incoming and outgoing parameters for a group of channels such as IP profiles, routing tables, and translation tables to be assigned during the configuration of the specific channel group.

To use a DS1 or E1, you must create at least one DS0 group for the DS1 or E1. The 5620 SAM supports the automatic configuration of sub-channels and assignment of timeslots on the ports within DS0 groups. Depending on the TDM port selected, the 5620 SAM automatically creates the DS0 channel groups with the appropriate type of timeslots. For example, you can assign timeslots to a DS0 channel group as follows:

- For DS1 channel types: Use four timeslots per channel group, which results in six DS0 channel groups with IDs from 1 to 6. Each contains four timeslots.
- For E1 channel types: Use five timeslots per channel group, which results in six DS0 channel groups with IDs from 1 to 6. Each contains five timeslots, with one timeslot not assigned.

You can view the channels that are assigned in DS0 groups using the associate properties form. You can also disable, enable, or reassign the assignment of timeslots as required, in a DS0 group.

See “TDM channelization and clear channel applications” in this section for more information about DS0 channel groups. See Procedure 20-36 for information about creating channels on ports for card types that support multiple sub-channels. See Procedure 20-41 for information about creating TDM DS1 or E1 channels and DS0 channel groups.

SONET STS-1 sub-channels

Only the DS0 group level can be used as a connection termination point for SONET STS-1 sub-channels. Channelization on the 1 × OC12 can be used to create up to 12 SONET STS-1 sub-channels. Each STS-1 channels can be used to create a DS3 frame on which you can build DS1 or E1 channels that can be configured to the DS0 channel group level. You can configure the DS0s of a DS0 group in any sequence and you do not need to use all DSOs. For example, you can use DS0 1, 3, 5, and 9. See “SONET VT1.5 and VT2 payloads” in this section for more information.

Only the DS0 group level can be used as an endpoint on the channelized 12 × DS3 card. Channelization can be used on each DS3 port of the card to create independent TDM channels in the form of DS1 or E1 data channels that handle DS0 groups. The DS0s of a DS0 group can be configured in any sequence and you do not need to use all DS0s. For example, you can use DS0 1, 3, 5, and 9. See “SONET and SDH sub-channel applications and structure” in this section for more information.

Ethernet ports

Ethernet ports can be configured as connection termination points in SAPs and IP interfaces. They cannot be channelized.

You must configure the class of port, such as fast Ethernet, Gigabit Ethernet, or 10G Ethernet. You must also configure the port encapsulation at the connection termination point. Ethernet access ports use:

- dot1q—supports multiple services on the port; the outer encapsulation value that distinguishes services is the VLAN ID in the IEEE 802.1Q header
- Q in Q—supports multiple services on the port/channel; the inner and outer encapsulation values that distinguish services is the VLAN ID in the IEEE 802.1Q header
- null—supports a single service on the port

You must configure the duplex parameter from the Ethernet tab if the port is to be added to a LAG. Configure the Dot1 Q Ethertype and Q in Q Ethertype parameters from the Ethernet tab, if required. The range is 1536 to 65 535.

You must also configure the speed parameter from the General tab. The options are 10, 100, 1000, or 10 000, depending on the speed of the Ethernet interface.

Most OmniSwitch chassis offer four hybrid or combo ports. These ports consist of four paired 10/100/1000Base-T ports and four 1000 SFP ports. Preferences for these ports are configurable and, depending on the configuration, redundancy can be provided if a link fails.

PoE is supported on the OmniSwitch, except for the Metro version of the OS 6250, and provides power directly from the Ethernet ports. Powered devices such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into the Ethernet ports. The powered devices receive both electrical power and data flow from the RJ-45 ports.

OmniSwitch learned port security

LPS provides a mechanism to control network device access on one or more OmniSwitch ports. Configurable LPS parameters allow you to restrict the source learning of host MAC addresses to:

- a specific amount of time in which the switch allows source learning to occur on all LPS ports
- a maximum number of learned MAC addresses allowed on the port
- a list of configured authorized source MAC addresses allowed on the port

The following options allow you to specify how the LPS port handles unauthorized traffic.

- Block only traffic that violates LPS port restrictions; authorized traffic is forwarded on the port.
- Disable the LPS port when unauthorized traffic is received; all traffic is stopped and a port reset is required to return the port to normal operation

See Procedure 31-54 for information about enabling LPS on Ethernet ports and configuring LPS properties. See Procedure 20-34 for information about configuring static MAC addresses on LPS enabled Ethernet ports

Note — A deployment error is displayed in 5620 SAM while creating a LAG with ports. This deployment failure occurs if there is an LPS/VLAN configuration done on a specific port, using CLI.

MTU size and port configuration

You must specify the MTU size for an Ethernet port using the MTU (bytes) parameter on the General tab at the connection termination endpoint.

Consider the following when you configure MTU parameters.

- The managed devices must handle MTU limitations at many service points. The physical (access and network) ports, service, and service tunnel MTU values must be individually defined.
- The ports to be designated as network ports and the ports to be designated as access ports intended to carry service traffic must be identified.
- MTU values should not be frequently modified.
- Service MTU values must be less than or equal to the service tunnel MTU.
- Service MTU values must be less than or equal to the access port MTU.
- The MTU value for an in-band management port should be less than or equal to the MTU value for the peer port connected to the in-band management port.

See the device specific documentation for end-to-end considerations for configuring maximum MTU size throughout the managed network.

The Ethernet port MTU parameter indirectly defines the largest physical packet that the port can transmit or that the far-end Ethernet port can receive. Packets received that are larger than the MTU are discarded. Packets that cannot be fragmented at egress and that exceed the MTU are discarded.

The parameters for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and complete Ethernet payload.

The MTU value for a port is associated with the port mode, such as access or network, and the port encapsulation type. If you change the mode or encapsulation type value for a port, the 5620 SAM adjusts the MTU value to a default value. If you do not want the MTU values for ports to revert to the defaults, you can configure the 5620 SAM to retain the currently configured MTU values for ports regardless of a mode or encapsulation type change. See Procedure 20-4 for more information.

HSMDA Egress Secondary Shapers

The egress port scheduler combines all subscriber queues of the same scheduling class and services the queues in a byte fair round robin fashion. This results in more packets being forwarded into the aggregation network towards a DSLAM than the DSLAM can accept. If the HSMDA egress port is congested, the egress bandwidth represented by the downstream discarded packets to the DSLAM may be allocated packets destined to other DSLAMs.

The HSMDA supports egress secondary shapers to provide a control mechanism to prevent downstream overruns without affecting the class-based scheduling behavior on the port. All subscribers destined to the same DSLAM have their queue groups mapped to the same egress secondary shaper. As the scheduler services the queues within the groups according to scheduler class, the destination shaper is updated.

After the shapers rate threshold is exceeded, scheduling for all queues associated with the shaper is stopped. When the dynamic rate drops below the threshold, the queues are allowed to be placed back on the scheduler service lists. By removing the queues from their scheduling context for a downstream congested DSLAM, the port scheduler is allowed to fill the egress port with packets destined to other DSLAMs without affecting class behavior on the port.

Egress secondary shapers are configured per port.

Moving and copying SAPs between ports

You can move and copy SAPs between physical Ethernet ports, logical ports, or a combination of both. You can also move and copy SAPs between endpoints configured with ATM encapsulation. For example, you can move a SAP on an IMA bundle to another bundle or to a TDM channel configured with ATM encapsulation. This functionality is typically used in redundancy scenarios, or to recover from a hardware failure.

Consider the following before you attempt to copy or move a SAP:

- Ports:
  - The source and destination ports can be on the same or different chassis. Inter-chassis copy or move is supported only when both NEs are of the same type, in the same chassis mode, and at the same major software release, for example, 8.0 R1 and 8.0 R3.
  - The source and destination ports can be the same. This configuration allows you to change the encapsulation values for a group of SAPs on the same port using outer and inner encapsulation offset values. These values can be positive or negative, depending on whether the encapsulation values must increase or decrease.
  - The physical Ethernet ports can be of different types; for example, Fast Ethernet (10/100/1000 Base-T), Gigabit Ethernet (1000 Base-T), and 10 Gigabit Ethernet (10 GBase-T).
  - The source and destination ports must be configured as access ports.
  - The encapsulation type must be the same on the source and destination ports.
  - You cannot copy or move a SAP between an HSMDA port and a non-HSMDA port.
- SAPs:
  - The SAPs can be associated with either L2 access interfaces on services such as Apipes, Epipes, Ipipes, VPLS, and MVPLS, or L3 access interfaces or subscriber interfaces that are associated with services such as IES and VPRN.
  - The copy and move operation does not copy and move MEPs that are configured on a VPLS, MVPLS and Epipe L2 access interface. MEP configuration is discarded during the copy and move operation.
  - For L2 and L3 access interfaces, you can move all SAPs or a subset of the SAPs on a port. You can also copy all SAPs or a subset of the SAPs on a port for L2 access interfaces.
  - All SAPs associated with a specific port within a group interface contained in an L3 subscriber interface can be moved at the same time.
  - The copy and move operations fail if the encapsulation value for a SAP on the source port is used by a SAP on the destination port. You can modify the SAP encapsulation values used on the destination port, if required.
  - The selected SAPs on the source port do not need to belong to the same service.
  - If a SAP on the source port belongs to a service not supported on the destination port, the SAP is not copied or moved.
  - The maximum number of SAPs varies for ports and MDAs. The SAP copy or move operation fails if the SAP capacity is exceeded for the destination port.
  - You cannot change SAP encapsulation from bridged to routed if ARP and DHCP options have been configured.
- SAP attributes:
  - VPLS and MVPLS dynamic FIB entries that are associated with copied or moved SAPs are discarded. Static FIB entries are transferred to the destination port after a successful SAP copy or move.
  - All SAP redundancy relationships at the source port, such as those provided by an MVPLS, are discarded during a copy or move operation.
  - All alarms, statistics, or OAM test results that are associated with a copied or moved SAP are discarded.

- When a source SAP belongs to an SHG, the 5620 SAM attempts to preserve the SHG membership. The destination SHG must have the same name as the source SHG, and must have the same residential SHG status. If an SHG with the same name does not exist on the destination service site, the 5620 SAM creates it.
- When a source SAP is uses an aggregation scheduler, the scheduler is copied to the destination. The aggregation scheduler must be unique to the destination NE and must have the same scope, for example, MDA or port.

See Procedures 20-5, 20-6, 20-7, and 20-8 to copy or move access interface SAPs between ports.

SONET/SDH and TDM port encapsulation

SONET/SDH and TDM ports can be configured as connection termination points in SAPs and IP interfaces. They can be channelized.

An access port is used for customer-facing traffic on which services are configured. SAPs can only use an access port. When a port is configured for access mode, the appropriate encapsulation type must be specified to distinguish the services on the port.

You must configure the Encap Type parameter from the General tab at the connection termination point. SONET/SDH or TDM ports or channels support the following encapsulation types, depending on the MDA type:

- BCP Null
- IPCP
- BCP Dot1 Q
- FR — Support multiple services using the DLCI header to distinguish services
- ATM — Support multiple services using the VCI or VPI of the PVC
- PPP Auto
- CEM

MTU size considerations apply to SONET/SDH and TDM channels. See “MTU size and port configuration” in section 20.2 for more information.

SONET clear channel applications

Ports on OC-*n* cards can be used for SONET clear channel applications. SONET or TDM clear channel applications allow you to create a full channel on a port which can be configured as access or network mode for SONET and access only for TDM. For example, when you create a 16 × OC3 SFP card, 16 ports are created. You can create one full channel on each of these ports. For more information about the 4-port OC3/STM1 ASAP SFP card for clear channel support on the 7705 SAR-8, see OC3/STM1 clear channel support on the 7705 SAR-8 in this section.

STS-192/48/12/3 clear channel applications use the following syntax:

```
card slot/daughtercard/port.STSType
```

For example, the clear channel STS-12 on slot 4, MDA 1, port 1 is named 4/1/1.sts12

Table 20-2 lists available SONET channel applications and parameters for clear channel, sub-channel, and TDM applications.

Table 20-2 SONET channel parameters

Applications	Channel ranges								
	STS-192	STS-48	STS-3	STS-1	DS3	DS1	DS0	E1	DS0
SONET Clear channel	1	1	1		1				
SONET Sub channel			1 to 4	1 to 3	1	1 to 28	1 to 24	1 to 21	2 to 32
TDM					1	1 to 28	1 to 24	1 to 21	2 to 32

OC3/STM1 clear channel support on the 7705 SAR-8

The 7705 SAR-8 supports the 4-port OC3/STM1 ASAP SFP card. The 4-port OC3/STM1 ASAP SFP card supports access mode for ATM-encapsulated traffic only. See ATM encapsulation in this section for more information. The interface must be configured as UNI.

All of the ports on this card can be independently configured for either SONET (OC3) or SDH (STM1) framing. The transmit clock rate for a port can be device- or loop-timed.

The section trace (J0) byte can be configured by the operator to check the physical cabling. The port can activate and deactivate local line and internal loopbacks. The MTU size for a 4-port OC3/STM1 ASAP SFP access port is fixed at 1572 for ATM encapsulation.

CSM activity switches for a 4-port OC3/STM1 ASAP SFP card on the 7705 SAR-8 are hitless on the data path.

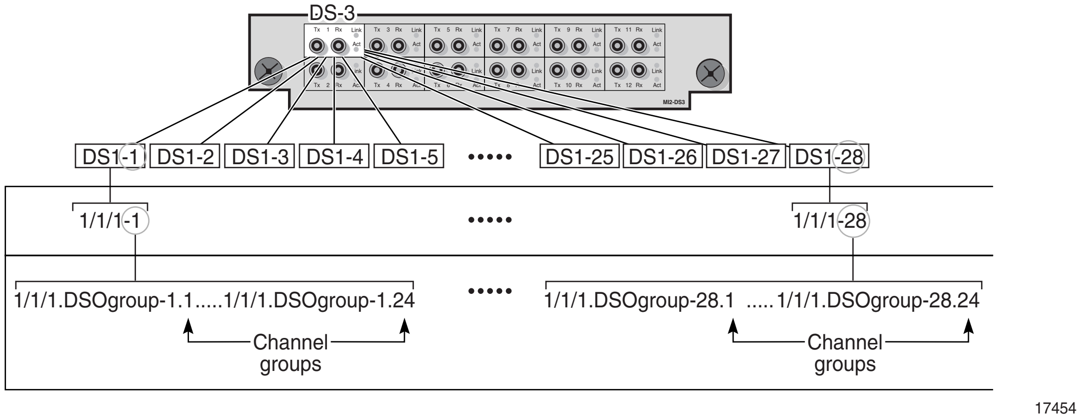
Note — Channels on the 4-port OC3/STM1 ASAP SFP adapter card cannot be configured as IES SAPs.

TDM channelization and clear channel applications

When you create a 4 or 12 ×DS3/E3 card, 4 or 12 DS3/E3 ports are created. You can then create DS3/E3 channels using the 5620 SAM, one per port. Each DS3/E3 channel can be channelized into 28 independent DS1 or 21 independent E1 data channels or, in clear channel applications, the DS3 can be the connection termination point. For channelized DS3 connections, each DS1 channel can be channelized to 24 DS0 groups and each E1 channel can be channelized to 31 DS0 groups. To use a DS1 or E1, you must create at least one DS0 group for the DS1 or E1.

By default, DS3 ports are automatically created for clear channel connections. To create a channelized DS3, you must configure the DS3 channel type as E3 or DS3 on the port. To channelize the DS3 to the DS0 level, you must set the Channelization Type to Channelized DS1 or E1. Figure 20-3 shows the channelized DS3 port structure for DS1 channels.

Figure 20-3 Channelized 12 × DS3 port structure for DS1 Channels



The channelized DS3 port structure for E1 channels has the following parameter values:

- each DS3 port supports 21 E1 channels
- each E1 channel supports 31 DS0 channel groups

TDM-based DS3 channelization uses the following syntax:

DS3 channel configured for TDM:

```
card slot/daughtercard/port.DS3-
```

DS1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[DS1#]
```

E1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[E1#]
```

DS0 group channel from the DS1 channel:

```
slot/daughtercard/port.DS0Grp-[STS3#].[STS1#].[DS1#/E1#].[Group#]
```

Table 20-3 provides an example of the naming conventions for a 12 × DS3 port.

Table 20-3 Example of TDM channel naming convention

Syntax	Description	Additional information
Channel 1/1/1.ds3	1/1/1 is the slot number/daughtercard number/port number .ds3 identifies the channel as DS3	Because DS3s are unchannelized by default, you must configure the Channelization Type as Channelized.
Channel 1/1/1.ds1-1.2	.ds1 identifies the channel as DS1 1 is the DS3 number .2 is the DS1 number (1 to 28)	Identifies the DS1 channel and shows how the DS3 level acts as a place holder for the DS1s.

(1 of 2)

Syntax	Description	Additional information
Channel 1/1/1.e1-1.2	.e1 identifies the channel as E1 1 is the DS3 number .2 is the E1 number (1 to 21)	Identifies the E1 channel and shows how the DS3 level acts as a place holder for the E1s.
Channel 1/1/1.ds0Grp-1.2.23	.ds0Grp- identifies the channel as a DS0 group 1 is the DS3 number .2 is the DS1 number (1 to 28) or E1 number (1 to 21) .23 identifies the DS0 channel group (1 to 24) on the DS1 or (2 to 32) on the E1	The DS0 group is configured on the DS1 or E1 channel. Only a DS0 can be used as a CTP.

(2 of 2)

ATM encapsulation

SONET/SDH clear channels can be provisioned so that ATM cells are encapsulated in SONET/SDH frames. The entire SONET/SDH path of the port is then used to carry ATM cells. The channel of the port becomes the ATM interface. ATM encapsulation is supported on the following daughter cards:

- 16 × ATM OC3 SFP
- 16 × ATM OC3 SFP B
- 4 × ATM OC12/OC3 SFP
- 4 × ATM OC12/OC3 SFP B
- 4 × OC3/STM1 ASAP SFP
- 4 × Any Service Channelized OC3
- 16 x Any Service Channelized DS1/E1

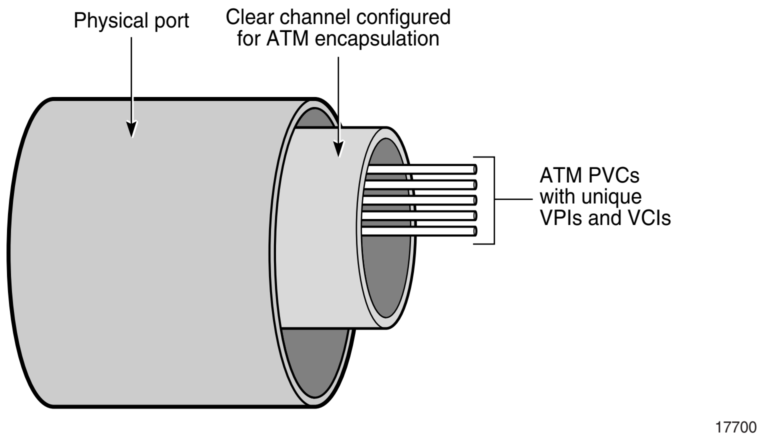
SONET/SDH clear channel applications with ATM encapsulation use the following syntax:

```
Daughter Card Slot - 3 (16 x ATMOC3), OK

Port 3/1/1 - Speed: OC3, State: OK

Channel 3/1/1.sts3, Mode: Access, Encap: ATM, State: Ok
```

Customer devices with ATM interfaces are connected directly or using the ATM access network to a 7750 SR that offers IES or VPRN services.

A SONET/SDH clear channel with ATM encapsulation can carry multiple ATM PVCs. ATM PVCs cannot be created from the 5620 SAM. They are created automatically by the router when a new Layer 3 interface over ATM is created. Figure 20-4 shows an example of ATM PVCs on a SONET/SDH clear channel.

Figure 20-4 ATM PVCs on a SONET/SDH clear channel



ILMI links between ATM interfaces

ILMI links can be configured between ATM interfaces. ILMI is a protocol that sets and sends physical layer, ATM layer, virtual path, and virtual channel parameters that are exchanged by ATM interfaces.

When ILMI is run between two ATM interfaces, the interfaces exchange ILMI packets that consist of SNMP messages across the physical connection. An ILMI link allows ILMI to run on an available virtual channel. When an ILMI link is created to carry ILMI messages, a PVC is automatically created with default PVC attributes. The PVC is deleted when the ILMI link is removed.

IMA

IMA is supported on channelized ASAP MDAs on the 7750 SR, 7710 SR, 7705 SAR, and ATM DS1/E1 CMA on the 7710 SR. IMA group bundles aggregate E1 or DS1 ATM paths into a single logical ATM interface. Each IMA group bundle can have from 1 to 8 members, or links. Up to 56 IMA group bundles can be configured on a single 7750 SR or 7710 SR MDA. Up to 8 IMA group bundles can be configured on a single 7705 SAR daughter card.

For the 9500 MPR, IMA is supported on the 16 x E1 ASAP Access (ETSI) card. Each IMA group bundle can have up to 16 links and there can be up to 8 IMA groups on a card.

Each ATM Interface supports up to 48 VP/VC connection points. Each 16 x E1 ASAP Access (ETSI) board supports up to 128 VP/VC connection points.

An IMA group bundle has the following common interface properties:

- ATM encapsulation type is displayed on the ATM Interface properties form by clicking on the “Edit ATM button”.
- The ATM interface characteristics can be viewed by clicking on the “Edit ATM button” button on the Bundle Properties form. This button is displayed on the Bundle Properties form only for the 9500 MPR.
- The interface mode is access only for the 9500 MPR.

- MTU value (of the primary link)

Note — The two following paragraphs do not apply to the 9500 MPR.

Member links inherit the common properties of the IMA group to which they belong. Only the properties of the primary link can be changed. The primary link is the member with the lowest interface index or initialization sequence. The primary link may change as member links are added and deleted from the IMA group.

Consider the following when you create a multilink IMA group bundle.

- When a path becomes a member of an IMA group bundle, it is no longer a physical ATM path interface.
- The members of the IMA group bundle inherit all of the properties of the primary link, such as the SONET configuration and MTU. If you modify the configuration of the primary link, the configuration of the bundle members is also modified.
- Member links that are added after the primary link has been added to the IMA group bundle must match the configuration of the primary link.
- You cannot configure services on a member link.

20.3 SONET and SDH sub-channel applications and structure

SONET sub-channel applications allow you to create multiple STS-1 channels on deep channelized OC-12 and OC-3 ports, and to configure multiple DS0 connection termination points.

An STS-1 sub-channel is configured, or channelized, to carry one of the following payload types:

- DS3
- VT1.5
- VT2

Because of the differences between SONET and SDH in multiplexing and mapping of tributary payloads into higher digital levels, some building blocks of SDH have no SONET equivalent and therefore the containment hierarchy and terminology for SDH is different from SONET. See “Comparison of SONET and SDH hierarchies” and “SDH AU-4 and AU-3 sub-channel applications” in this section.

SONET DS3 payload

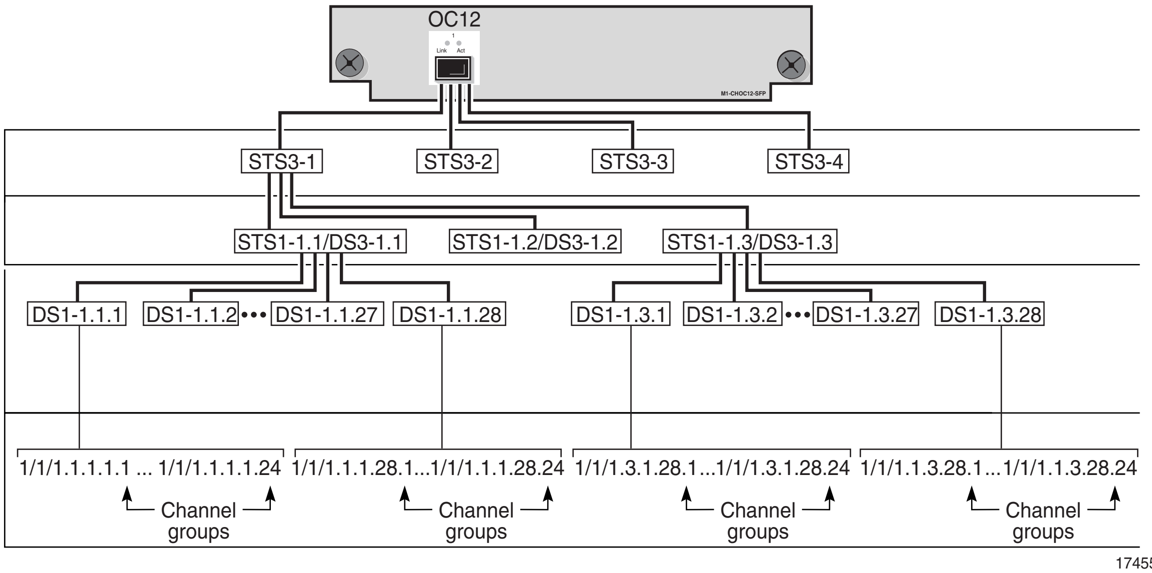
The following example, illustrated in Figure 20-5, shows the channelization sequence for a DS3 payload on a 1 × OC12 Deep Channel card.

1. One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.
2. This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to carry a DS3 frame

4 Each DS3 frame can be channelized into 28 independent DS1 data channels or 21 independent E1 data channels. Each channel must be created one at a time.

Figure 20-5 Channelized 1 × OC-12 port structure using STS-1/DS3 sub-channels



SONET VT1.5 and VT2 payloads

The following example, illustrated in Figure 20-6, shows the channelization sequence for a VT1.5 or VT2 payload on a 1 × OC12 Deep Channel card.

1 One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.

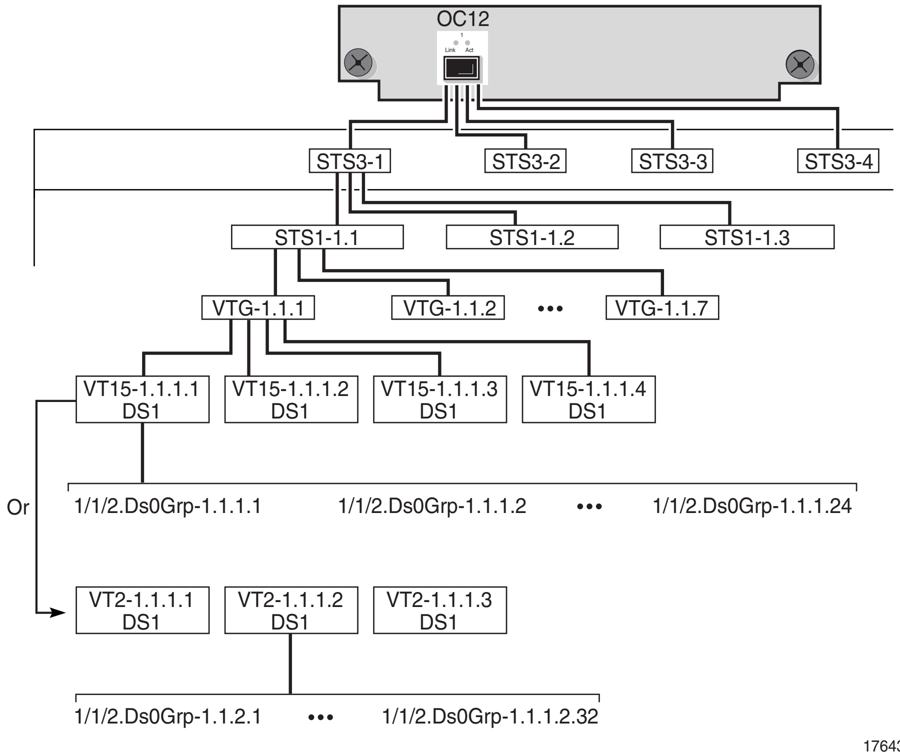
2 This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to be channelized to carry up to 28 DS1. For SONET sub-channel configuration you must select payload type VT1.5 or VT2. When you choose VT1.5 payload type, seven VTG are implicitly created.

4 Each VTG is channelized into four independent VT1.5 channels or three VT2 channels, each of which can carry an independent DS1 data channel. Each channel must be created one at a time.

5 Each VT1.5 DS1 channel can be configured to handle up to 24 DS0 groups. Each VT2 DS1 channel can be configured to handle up to 32 DS0 groups. To use a DS1, you must create at least one DS0 group for the DS1 or E1.

Figure 20-6 Channelized 4 × OC-3 port structure using VT sub-channels



SONET sub-channel syntax

The 5620 SAM uses the following SONET syntax for the STS-1 sub-channel:

```
card slot/daughtercard/port.STS1-[STS3#].[STS1#]
```

DS3 channels from an STS-1 sub-channel use the following syntax:

```
slot/daughtercard/port.DS3-[STS3#].[STS1#]
```

DS1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[DS1#]
```

E1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[E1#]
```

VT15 or VT2 from a VT group use the following syntax:

```
slot/daughtercard/port.VTG#-[STS3#].[STS1#]
```

DS1 channels from a VT15 or VT2 use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[VT15#] or
[VT2#}.[VTG#].[DS1#]
```

Table 20-4 shows an example of the SONET sub-channel syntax.

Table 20-4 Example of SONET sub-channel syntax for an OC-12 port

Syntax	Description	Additional information
Channel 1/1/1.sts1-2.2	1/1/1 is the slot number/daughtercard number/port number 2 is the STS-3 number (1 to 4) .2 is the STS-1 number (1 to 3)	The sts1 parameter is 2.2 which means that it is the fifth STS-1. There are four STS-3s for an OC-12 and each STS-3 has three STS-1s such that the fifth STS-1 is the second STS-1 of the second STS-3.
Channel 1/1/1.ds3-2.2	.ds3-2 is the STS3 number (1 to 4) .2 identifies the STS-1 number (1 to 3)	Identifies the DS3 channel and shows how the sts1 level acts as a place holder for the DS3
Channel 1/1/1.ds1 2.2.25	.ds1-2.2.25 identifies a DS1 channel (1 to 28) on the DS3	The DS1 is configured on the DS3.
Channel 1/1/1.e1 2.2.21	.e1-2.2.21 identifies a E1 channel (1 to 21) on the DS3	The E1 is configured on the DS3.
Channel 1/1/1.DS0Grp-2.2.20.5	.DS0Grp-2.2.20.5 identifies one of the DS0 channel groups: 1 to 28 for DS1; 2 to 32 for E1	The DS0 is configured on the DS1 or E1 channel.
Channel 1/1/1.ds1 2.2.3.18	ds1 2.2.3.18 identifies a DS1 channel on the VT15 or VT2 payload, where 3 is the VT group.	—

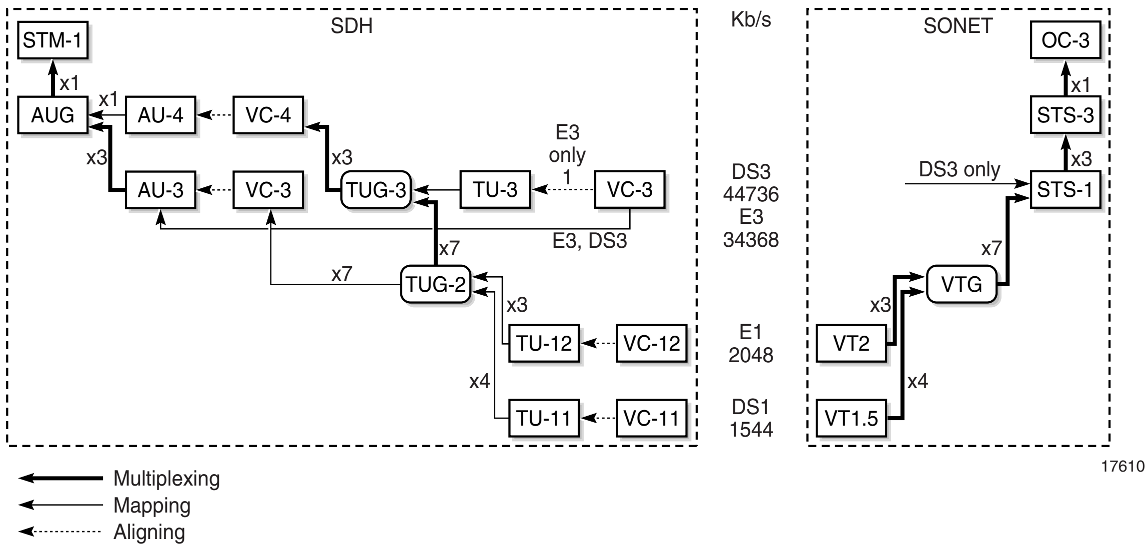
Comparison of SONET and SDH hierarchies

SONET and SDH are compatible digital hierarchies that support identical transmission rates with similar framing structures. However, SONET and SDH standards differ in the way they multiplex and map tributary payloads into higher digital levels. Because of these differences, some SDH framing blocks do not have equivalent blocks in SONET.

SONET provides one STS sub-channel, the STS-1, for mapping lower-capacity, deep-channel payloads while SDH provides two alternative sub-channels, the AU3 and the AU4. After an AU3 sub-channel is created, an AU4 cannot be created on that port in the case where the port is an OC-3 (STM-1). Conversely, if an AU4 sub-channel is created, an AU3 cannot be created on that port in the case where the port is an OC-3 (STM-1).

SONET and SDH transmission rates converge at 155.520 Mb/s where the SONET STS-3c is equivalent to the SDH STM-1 bit rate. For lower-capacity payloads, such as DS1, E1, DS3, and E3, SONET provides one unique mapping path for each payload while SDH permits two alternative paths for each payload as shown Figure 20-7.

Figure 20-7 Supported SONET/SDH multiplexing structures



SDH AU-4 and AU-3 sub-channel applications

SDH sub-channel applications allow you to create AU4 or AU3 channels on deep channelized OC-12 (STM-4) and OC-3 (STM-1) ports, and to configure multiple DS0 connection termination points.

After an AU4 sub-channel is created, it implicitly contains three TUG-3 groups. A TUG-3 is channelized to carry one of the following payload types:

- TU3
- TU11
- TU12

After an AU-3 sub-channel is created, it is channelized to carry one of the following payload types:

- DS3, E3
- TU11
- TU12

SDH TU3 payload

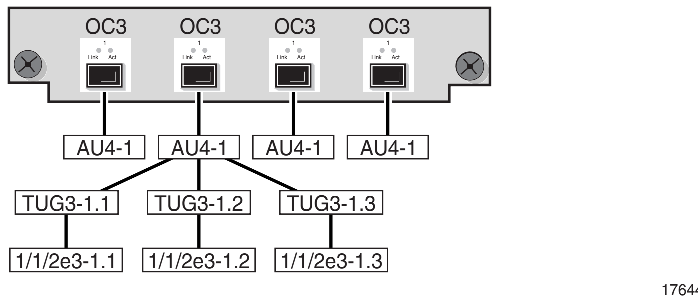
The following example, illustrated in Figure 20-8, shows the channelization sequence for a TU3 payload on a 4 × OC3 Deep Channel card.

1. Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.
2. The user creates each required AU4 sub-channel.
3. Each AU4 sub-channel implicitly contains three TUG3 groups.

4 You can then configure each TUG3 to carry a TU3 frame

5 Each TU3 frame is channelized into an independent E3 data channel and cannot be changed.

Figure 20-8 Channelized 4 × OC-3 port structure using AU4/TU3 sub-channels



SDH E3 or DS3 payload

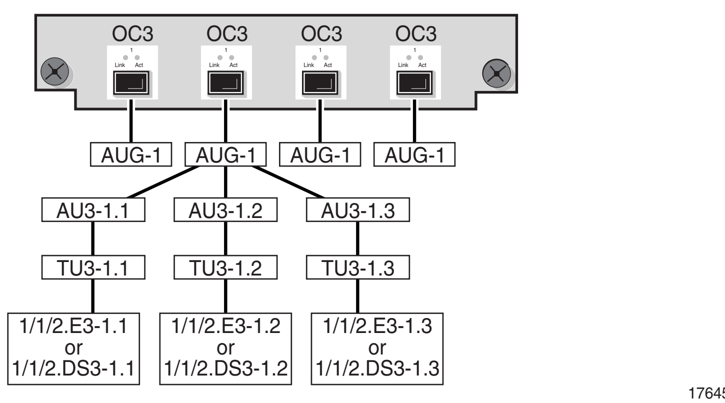
The following example, illustrated in Figure 20-9, shows the channelization sequence for an E3 or DS3 payload on a 4 × OC3 Deep Channel card using AU3 sub-channels.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

2 Each port can be channelized into up to three AU3 sub-channel.

3 Each AU3 frame can be channelized into an independent E3 or DS3 data channel.

Figure 20-9 Channelized 4 × OC-3 port structure using AU3/E3 sub-channels



SDH TU11 and TU12 payloads

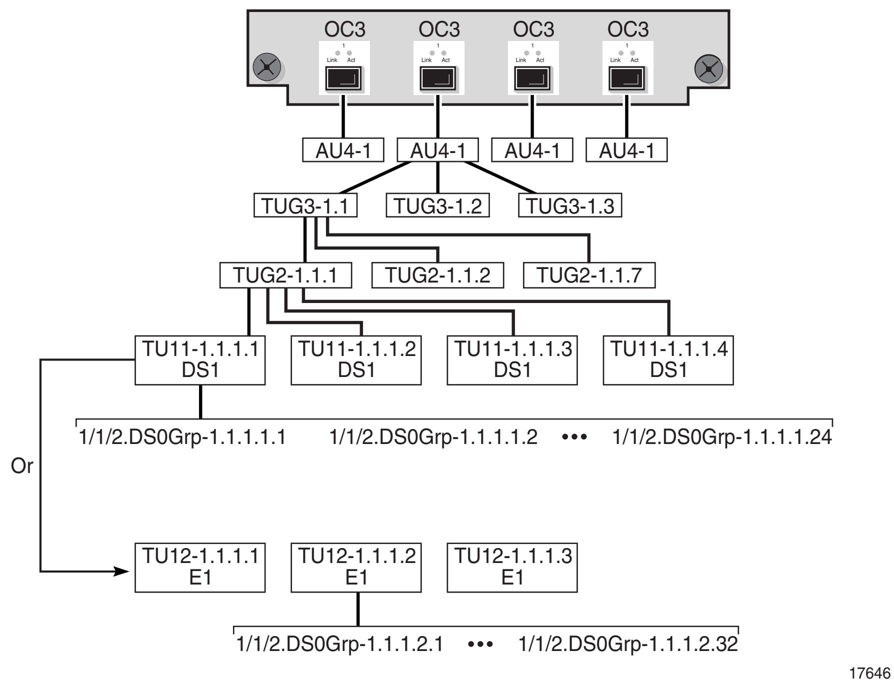
TU11 and TU12 payloads can be channelized using an AU4 sub-channel or an AU-3 sub-channel. An AU4 sub-channel implicitly contains three TUG3 groups. A TUG3 and an AU3 channelized to carry TU11 or TU12 payloads implicitly contain seven TUG2 tributary groups.

The following example, illustrated in Figure 20-10, shows the channelization sequence for a TU11or a TU12 payload on a 4 × OC3 Deep Channel card.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.
2 Each port can be channelized into one AU4 sub-channel or three AU3 sub-channels.
3 Each AU4 sub-channel implicitly contains three TUG3 groups.
4 You can then configure each TUG3 group or each AU3 sub-channel to carry a TU11 or TU12 payload.
5 Each TUG3 group or AU3 sub-channel implicitly contains seven TUG2 tributary groups.
6 Each TUG2 group can be channelized into three independent TU12 channels or four independent TU11 channels.
7 Each TU12 can contain an E1 or DS1 data signal. Each TU11 can contain a DS1 data signal. Each E1 can be configured to handle up to 31 DS0 groups. Each DS1 can be configured to handle up to 24 DS0 groups. To use an E1 or a DS1, you must create at least one DS0 group for the DS1 or E1.

Note — On the same TUG3 or AU3, you cannot mix TU-1*X* with DS1 and E1 payload types. Every TU-1*X* on the same TUG3 or AU3 must use the same payload type, either E1 or DS1, not a mix of both. The mix is shown in for illustrating the structure.

Figure 20-10 Channelized 4 × OC-3 port structure using AU4/TU sub-channels



20.4 Workflow to manage port objects

The following workflow describes the sequence of high-level tasks required to manage and configure port objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — After they are configured, port objects can be accessed using the equipment navigation tree. See chapter 4 for more information about using the equipment navigation tree.

1. As required, configure Ethernet ports. See Procedure 20-1 for more information.
2. As required, change the port mode. See Procedure 20-2 for more information.
3. As required, migrate SAPs from access mode to hybrid mode. See Procedure 20-3 for more information.
4. As required, configure the 5620 SAM to retain non-default port MTU values. See Procedure 20-4 for more information.
5. As required, copy or move L2 access interface SAPs between ports. See Procedure 20-5 for more information.
6. As required, move L3 access interface SAPs within or between ports on the same NE. See Procedure 20-6 for more information.

7 As required, move L3 subscriber interface SAPs between ports on the same NE. See Procedure 20-7 for more information.

8 As required, copy L3 access interface SAPs between ports on the same NE. See Procedure 20-8 for more information.

9 As required, add a queue group to an Ethernet port. See Procedure 20-9 for more information.

10 As required, configure SONET ports. See Procedure 20-10 for more information.

11 As required, configure an HSMDA port scheduler override. See Procedure 20-11 for more information.

12 As required, configure TDM DS3 ports. See Procedure 20-13 for more information.

13 As required, configure serial ports. See Procedure 20-13 for more information.

14 As required, configure ports on 7210 SAS devices, as follows:

- **a** Configure a 7210 SAS-M channelized TDM DS1 or E1 port; see Procedure 20-14 for more information
- **b** Assign policies to a 7210 SAS Ethernet port. See Procedure 20-15 for more information.
- **c** Configure an SHG for 7210 SAS NEs. See Procedure 20-16 for more information.

15 As required, configure ports on 7250 SAS devices, as follows:

- **a** 7250 SAS CES TDM DS1 or E1 port; see Procedure 20-17 for more information
- **b** Telco and 7250 SAS uplink ports as network ports; see Procedure 20-18 for more information

16 As required, configure a 7705 SAR ASAP channelized TDM port. See Procedure 20-19 for more information.

17 As required, configure a 7710 SR channelized TDM DS1 or E1 port. See Procedure 20-20 for more information.

18 As required, configure ports on 9500 MPR devices:

- **a** 9500 MPR Ethernet ports; see Procedure 20-21 for more information
- **b** ports on a 2xSTM card for 9500 MPR; see Procedure 20-22 for more information
- **c** ports on a 1xSTM Channelized card for 9500 MPR; see Procedure 20-23 for more information
- **d** 9500 MPR E1 and DS1 ports; see Procedure 20-24 for more information
- **e** 9500 MPR DS3 ports; see Procedure 20-25 for more information
- **f** 9500 MPR radio modem ports; see Procedure 20-26 for more information

19 As required, configure the following on 9500 MPR devices:

- **a** 9500 MPR port segregation; see Procedure 20-27 for more information
- **b** analog performance management on 9500 MPR radio modem ports; see Procedure 20-28 for more information
- **c** power source type on 2+2 x Ethernet (EAS) card slots for 9500 MPR; see Procedure 20-29 for more information
- **d** power level performance management on 9500 MPR radio modem ports. See Procedure 20-30 for more information.
- **e** add 9500 MPR port protection; see Procedure 20-31 for more information.
- **f** loopback test on a 9500 MPR DS1, ES1, or radio modem port; see Procedure 20-33 for more information

20 As required, configure OmniSwitch Ethernet ports. See Procedure 20-34 for more information.

20.5 Workflow to manage channel objects

The following workflow describes the sequence of high-level tasks required to manage and configure channel objects. This workflow assumes that the physical devices have been installed, commissioned, and discovered, and that the port objects have been configured. See chapter 13 for more information about device commissioning. See chapter 14 for more information about device discovery.

Note — After they are configured, channel objects can be accessed using the equipment navigation tree. See chapter 4 for more information about using the equipment navigation tree.

1 As required, configure SONET clear channels. See Procedure 20-35 for more information.

2 As required, create channels on ports for card types that support multiple sub-channels. See Procedure 20-36 for more information.

3 As required, configure SONET sub-channels. See Procedure 20-37 for more information.

4 As required, configure SDH sub-channels. See Procedure 20-38 for more information.

5 As required, create VT15 (TU11) or VT2 (TU12) sub-channels. See Procedure 20-39 for more information.

6 As required, create TDM DS1 channels. See Procedure 20-42 for more information.

7 As required, configure TDM DS1 or E1 channels. See Procedure 20-41 for more information.

8 As required, configure serial channels. See Procedure 20-42 for more information.

9 As required, create TDM DS3 channels. See Procedure 20-43 for more information.

10 As required, configure TDM DS3 channels. See Procedure 20-44 for more information.

11 As required, configure a DS3 or E3 channel as a network interface on a channelized ASAP MDA. See Procedure 20-45 for more information.

12 As required, configure an L3 interface on a DS3 or E3 channel on a channelized ASAP MDA. See Procedure 20-46 for more information.

13 As required, configure a PVC. See Procedure 20-47 for more information.

14 As required, create an ILMI link. See Procedure 20-48 for more information.

15 As required, modify an ILMI link. See Procedure 20-49 for more information.

20.6 Port configuration procedures

Use the following procedures to manage ports using the navigation tree.

Procedure 20-1 To configure Ethernet ports

Perform this procedure, as required, depending on the daughter card and port type that you are configuring. Different card types display different port configuration parameters.

Note — Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the device and an 802.1X policy must be created and distributed to the device.

See Procedure 17-6 in chapter 17 for information about enabling 802.1X on a device. See chapter 54 for information about creating and distributing 802.1X policies.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an Ethernet port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Configured MAC
- Mode
- L2Uplink
- Encap Type
- Speed
- MTU (bytes)
- DDM Event Suppression
- Hold Time Up (seconds)
- Hold Time Down (seconds)
- Load Balance Algorithm
- Ingress Percentage of Rate (%)
- Egress Percentage of Rate (%)
- Default VLAN
- Channel
- Rx Decision Threshold Voltage Adjustment
- Optical Transport Channel Unit
- OLC State

Only one MAC address can be assigned to a port. When a new MAC address is configured while the port is operational, IP issues an ARP, if appropriate, and BPDUs are sent with the new MAC address. A default MAC address is assigned by the system.

If the port is a LAG member, the Hold Time Up (seconds) parameter is configurable only if the port is the primary member. The Hold Time Down (seconds) parameter is not configurable when the port is a LAG member.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

6 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Ingress Buffer Allocation panel. Otherwise, go to step 9:

- Access Weight
- Network Weight

7 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Egress Buffer Allocation panel:

- Access Weight
- Network Weight

8 If you change the Mode parameter from Access to Hybrid and there are SAPs on the port, perform Procedure 20-3 to migrate the SAPs.

9 If you are configuring a 7210 SAS Ethernet port you can add the port to an SHG. See Procedure 20-16 for information about creating a 7210 SAS SHG.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port list form opens.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group - Physical Port list form closes, and the Physical Port (Edit) form refreshes with the SHG name.

Note 1 — A port cannot be added to or deleted from an SHG if it has a SAP configured on it or is a member of a LAG.

Note 2 — A port cannot belong to more than one SHG; you must remove any SHGs from the port before you can add the port to a different SHG.

10 Configure the Named Pool Buffer Policy for the port.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. A Select Ingress Pool Policy window opens with a list of ingress pool policies.

ii Choose a policy from the list.

iii Click on the OK button, the Select Ingress Pool Policy window closes and the Name parameter refreshes with the selected policy.

iv Configure the Ingress Percentage of Rate (%) parameter.

v Click on the Select button beside the Name parameter in the Egress Pool Policy panel. A Select Egress Pool Policy window opens with a list of egress pool policies.

vi Choose a policy from the list.

vii Click on the OK button, the Select Egress Pool Policy window closes and the Name parameter refreshes with the selected policy.

viii Configure the Egress Percentage of Rate (%) parameter.

Note — Ensure that the named pool mode is enabled. See Procedure 19-18 in chapter 19 for more information.

11 Click on the States tab button.

12 Configure the Administrative State parameter.

13 Click on the Policies tab button. The Policies form opens with the General tab displayed.

Note — The types of policies that you can choose depend on the type of NE, daughter card, and the mode type of the port you are configuring.

- The Network Queue and Accounting Policies panel are only displayed for network ports.
- The Port Scheduler panel is only displayed for ports on non-HSMDA daughter cards.
- The HSMDA Egress Scheduler panel is only displayed for ports on HSMDA daughter cards.

14 Click on the Select button in the Accounting Policy panel to assign an accounting policy to the port, if applicable. The Select Accounting Policy - Physical Port form opens.

15 Choose an accounting policy from the list and click on the OK button. The Select Accounting Policy - Physical Port form closes.

16 Configure the Collect Accounting Statistics parameter, and if required.

17 If you are configuring a 7210 SAS Ethernet port, perform Procedure 20-15. Otherwise continue to step 18.

18 Click on the Select button in the Network Queue panel to assign a network queue policy to the port, if applicable. The Select Network Queue Policy - Physical Port form opens.

19 Choose a network queue policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

20 Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port, if applicable. The Select Port Scheduler Policy - Physical Port form opens.

21 Choose a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

22 Click on the Select button in the HSMDA Egress Scheduler Policy panel to assign a scheduler policy to the port, if applicable. The Select HSMDA Egress Scheduler Policy - Physical Port form opens.

23 Choose a policy from the list and click on the OK button. The Select HSMDA Egress Scheduler Policy - Physical Port form closes.

24 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

25 Configure the parameters:

- Auto-negotiate
- Duplex
- Dot1 Q Ethertype
- Q in Q Ethertype
- Ingress Rate ()
- Egress Scheduler Mode
- CFM LoopBack Mode
- Egress Rate (Kbps)
- Egress Max-Burst
- Flow
- Ethernet Down Reason
- Down When Looped
- Down On Internal MAC Tx Error
- IP MTU (bytes)
- Port Clock Mode
- Retry Timeout (Sec)
- XGig Mode
- Forward All Multicast Traffic
- Forbid IGMP Snooping
- Backpressure
- Broadcast Limit (Pkts/s)
- Detect Remote Faults
- Detection
- Keep Alive Interval (Sec)
- Single Fiber
- Type
- Time (seconds)
- Swap MAC Address
- Synchronous status messages
- SSM Code-Type
- Tx DUS/DNU

The Dot1 Q Ethertype and Q in Q Ethertype parameters are not configurable for the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices. The XGig Mode parameter is only configured for 1 x 10-Gig and 12 x 10-Gig Ethernet interfaces, and is used to treat the port as a WAN-PHY interface, which encapsulates Ethernet frames over SONET.

The Flow parameter is configurable on Telco devices when the Auto-negotiate parameter is set to False.

In the Ethernet Down Reason parameter, the No Service Port option is available only for 7210 SAS-M NEs. The No Service Port applies to BOF which can be configured using CLI. These two ports cannot be used for user traffic. This is a read-only check box which indicates that the ports are down because it was classified as “No Service Port”.

The Backpressure, Broadcast Limit (Pkts/s), Detect Remote Faults, Detection, Forward All Multicast Traffic, and Forbid IGMP Snooping parameters are only configurable on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA.

The Keep Alive Interval (Sec) and Retry Timeout (Sec) parameters are only displayed when the Down When Looped parameter is enabled.

The Single Fiber parameter is configurable for 1 and 10 Gigabit Ethernet network ports on the 7750 SR and 7450 ESS, and is supported only on the 2 x XP MDA IOM 3 and IMM.

The Auto-negotiate and Duplex parameters are not supported on the 3-port 40GE QSFP IMM.

The Type and Time (seconds) parameters in the Timed Loopback panel are configurable only on Ethernet ports on the 7705 SAR, Release 2.1 or later.

Note — Management connectivity between the 5620 SAM and the 7705 SAR may be lost if a line loopback is applied to an Ethernet port that is carrying in-band management traffic. The line loopback remains in effect until the timer expires and the 7705 SAR removes the loopback.

26 To configure CRC threshold parameters, perform the following steps:

i Remove the check mark from the Disable check box and configure the CRC SD Threshold and CRC SD Threshold Multiplier parameters.

ii Remove the check mark from the Disable check box and configure the CRC SF Threshold and CRC SF Threshold Multiplier parameters.

iii Configure the Down On Internal MAC Tx Error parameter.

27 If the port is an access or hybrid port with Q in Q or dot1q encapsulation, the MEPs tab is displayed. Click on the MEPs tab button to add a facility MEP, if required and perform the following steps.

Note — Only one facility MEP can be configured on a port.

i Click on the Create button. The MEP (Create) form opens on the General tab.

ii Click on the Select button to choose a global MEG. The Select Maintenance Entity Group form opens.

iii Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

iv Configure the parameters:

- Auto-Assign ID
- CCM Messages Enabled
- Description
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)
- Facility Fault Notify

Note — To enable fault propagation on a facility LAG MEP, Facility Fault Notify must be enabled.

v If the MD for the MEP has a Name Type of none the Y.1731 Tests tab is configurable; click on the Y.1731 Tests tab button. Otherwise, go to step vii.

vi Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The MEP (Create) form closes.

28 Click on the 802.3ah tab button to configure and initiate the 802.3ah EFM OAM diagnostic as described in Procedure 38-48. Otherwise, continue to step 29.

29 Click on the 802.1x Port tab button, if required.

30 Configure the parameters:

- Initialize
- Reauthenticate Control

Note — You cannot configure the parameters for the 7710 SR.

31 Click on the 802.1x Port Authenticator tab button, if required. You cannot configure the parameters for the 7710 SR.

32 Configure the parameters:

- Controlled Port Control
- Quiet Period
- Tx Period
- Supplicant Timeout
- Server Timeout
- Max Req
- Reauth Period
- Reauth Enabled

33 Click on the Select button to choose a RADIUS policy. The Select Policy - Physical Port form opens.

34 Choose a RADIUS policy in the list and click on the OK button. The Select Policy - Physical Port form closes and the Physical Port (Edit) form displays the RADIUS policy name.

35 Go to Procedure 20-9 to add a queue group to the port.

36 If the port is an HSMDA access port, the Egress Secondary Shapers tab button is present. Click on the Egress Secondary Shapers tab button to add an egress secondary shaper to the port, if required, and perform the following steps.

Note 1 — An HSMDA port is initially created with a default egress secondary shaper. The default shaper cannot be deleted, but it can be modified.

Note 2 — Non-default egress secondary shapers can only be created if the port's Mode parameter is not set to the network option.

Note 3 — You cannot switch the Mode of an HSMDA port to network if there are non-default egress secondary shapers on that port. An error message will be issued. You must delete any non-default egress secondary shapers from the port before switching its Mode to network.

i Click on the Create button. The HSMDA Egress Secondary Shaper (Create) form opens, with the General tab displayed.

ii Configure the parameters:

- Name
- Low Burst Max Class
- Rate (Mbps)
- Monitor Threshold (Kbytes)
- Low Burst Limit
- High Burst Increase

The Rate (Mbps) parameter can only be configured if the associated MAX check box is not enabled.

iii Click on the Classes tab button.

iv Configure the Class Rate (kbps), Class Monitor Threshold (Kbytes) and Class Burst Threshold (bytes) parameters for Classes 1 through 8, as required.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new entry appears in the list.

37 Click on the LLDP tab button, if required. The LLDP configuration form opens with the Nearest Bridge sub-tab displayed.

38 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs

39 Repeat step 38 for the Nearest Non TPMR and Nearest Customer sub-tabs under the LLDP tab, as required.

40 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers associated with the port. These remote peers are used to determine the physical topology of the network.

41 The Access Group tab is present if the port is on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device. Click on the Access Group tab, if required. Otherwise, go to step 57.

42 Click on the Create button to create an access group, or select an existing access group in the list and click on the Properties button. The Port Access Group (Create) form opens.

43 Configure the parameters:

- Displayed Name
- Description
- Type

44 Click on the OK button. A dialog box appears.

45 Click on the OK button. The new access group appears in the list.

46 The QoS tab is present if the port is on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device. Click on the QoS tab button, if required. Otherwise, go to step 58.

47 Click on the Create button to configure QoS settings for the port. The QoSPort (Create) form opens.

48 Configure the parameters:

- Displayed Name
- Description
- Priority
- Queue Algorithm
- Drop Algorithm
- Shaper Rate

49 Click on the OK button. A dialog box appears.

50 Click on the OK button. The new QoS entry appears in the list.

51 Click on the Qos Pool tab button, if required.

52 Choose a QoS pool from the list and click on the Properties button. The QoS Pool (Edit) form opens.

53 Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

54 Choose a slope policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes and the QoS Pool (Edit) form refreshes with the name of the slope policy.

55 Configure the parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

56 Click on the OK button. The QoS Pool (Edit) form closes.

57 Perform one of the following:

a Click on the Override Policy Items tab button to configure HSMDA overrides. See Procedure 20-11 for more information.

b Continue to step 58.

58 To configure a 1x10-Gig Ethernet DWDM tunable optics MDA or a 1-Port OC768 OTU3 Long Reach DWDM Tunable IMM on a 7750 SR or 7450 ESS, click on the Optical Transport Channel Unit tab button. Otherwise, go to step 70.

59 Configure the following parameters on the General tab:

- FEC Mode
- SF-SD Method
- SF Threshold (10E-n bits received)
- SD Threshold (10E-n bits received)
- Configured Data Rate (Gb/s)
- Transmitter Mode
- Transmitter String
- Async Mapping
- Transmitter Bytes
- Expected Rx Mode
- Expected Rx String
- Expected Rx Bytes
- OTU-TIM reaction
- ODU-TIM reaction
- OPU-TIM reaction
- Payload Type (hex)
- Expected Payload Type (hex)
- OPU-PLM reaction

60 Click on the OTU Alarms tab button and select the OTU alarms for the Configured Alarms parameter.

61 Click on the Select button in the DWDM panel to choose a channel. The Wave Length Reference - Physical Port form opens.

62 Use the configurable filter and click on the Search button to generate a list of configurable channels and related wavelengths and frequencies.

63 Select a channel and click on the OK button. The Wave Length Reference - Physical Port form closes and the channel number, wavelength, and frequency are displayed in the DWDM panel of the Physical Port (Edit) form.

64 Click on the Optical tab button and configure the following parameters on the Wavelength Track tab:

- Wave Tracker Encode
- Wave Tracker Power Control
- Configured Alarms
- Wave Key1
- Wave Key2
- Target Power

65 Click on the Optical Amplifier tab button and configure the Configured Alarms parameter.

66 Click on the Optical Tunable Dispersion Compensation Module tab button.

67 Configure the following parameters:

- Channel
- Dispersion
- Control Mode
- Configured Alarms

68 Click on the Apply button. A dialog box appears.

69 Click on the Yes button.

70 Click on the other tab buttons to view and edit additional port information.

71 Click on the Cancel if no changes were made, otherwise click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-2 To change the port mode

Perform this procedure to change the port mode between Network and Access modes.

Note — Save the device configuration before you perform this procedure. See the appropriate NE documentation for more information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to change the port mode and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port. The Physical Port (Edit) form opens with the General tab displayed.

5 Change the Mode parameter as required and click on the Apply button.

6 If you are changing the mode from Access to Network and there are services configured on the port, one of two warnings is presented in a dialog box, depending on the permissions associated with your user role.

a The default warning dialog indicates that the object has dependencies that will be deleted if you apply the port mode change.

i Click on View Dependencies button to see the number of dependencies (services and interfaces) associated with the port.

ii Click on the OK button.

iii Confirm that you understand the implications of changing the port mode by enabling the “I understand the implications of this action” check box. A confirmation dialog box appears.

iv Click on the Yes button. Any services and interfaces associated with the port, including SAPs, are deleted, and the mode for the port is changed to Network.

Note — Changing the port mode from Access to Network without first removing the dependencies results in a TopologyMisconfigured alarm.

b For users who have the port.RestrictNodeConfigModify permission associated with their role, a warning form appears, indicating that the object has dependencies that must be removed before proceeding.

i Click on View Dependencies button to see the number of dependencies (services and interfaces) associated with the port.

ii Click on the OK button.

iii Remove the services or interfaces associated with the port. You can manually delete them or move them to other ports as described in this chapter.

iv Repeat steps 3 to 5 to change the port mode to Network.

Procedure 20-3 To migrate SAPs from access mode to hybrid mode

Perform this procedure on Ethernet or SC-LAG access ports that contain SAPs.

Note — Save the device configuration before you perform this procedure. See the appropriate NE documentation for more information.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to migrate SAPs and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on an Ethernet port or SC-LAG port. The Physical Port (Edit) form opens with the General tab displayed.

5 Change the Mode parameter from Access to Hybrid. A dialog box opens.

6 Click on the Yes button. A warning form appears, stating that you must perform an admin save.

7 Perform Procedure 23-4 in response to the warning form.

8 Select the I understand the implications of this action check box and click on the Yes button. The SAP Migration Result window displays information about the number of SAPs migrated.

9 Click on the OK button to close the windows.

Procedure 20-4 To configure the 5620 SAM to retain non-default port MTU values

Use this procedure to configure a 5620 SAM server for non-default MTU refresh behavior.

Note — If the 5620 SAM system is deployed in a redundant configuration, you must perform this procedure on each main server in the 5620 SAM server cluster.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Open the nms-server.xml file with a plain-text editor.

4 Add the following line to the end of the file:

```
<customMTURefresh refresh="true"/>
```

5 Save the nms-server.xml file.

6 Close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the console prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM server reads the nms-server.xml file and puts the configuration change into effect.

10 Close the console window.

Procedure 20-5 To copy or move L2 access interface SAPs between ports

Note — In this release, you cannot move or copy an MSAP.

You can also use the 5620 SAM clipboard functionality to copy or move SAPs. See chapter 3 for information about using the 5620 SAM clipboard.

1 For the source NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

2 On the source NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation

Caution — An unsuccessful SAP copy or move may result in the deletion of one or more source SAPs from the source NE. The backed-up configuration file is required to restore the configuration on the source NE if a SAP copy or move operation fails.

See the appropriate device documentation for more information about saving the device configuration to a file.

3 For the destination NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

4 On the destination NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

5 Open the Deployment form to monitor deployments as they occur during the SAP copy or move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP copy or move operation to ensure that faults that may arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the copy or move operation.

6 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

7 Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the Alarm window are all shown.

8 Click on the Result Export Path tab button. The Result Export Path form opens.

9 Specify the file name and location in which to save a text file that contains the results of the SAP copy or move operation.

10 Click on the Set button. The Result Export Path form closes.

11 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

12 Choose a source NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

13 Click on the Select button beside the Source Port parameter. The Select Port form opens.

14 Configure the filter criteria. A list of available ports is displayed.

15 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

16 Click on the Select button beside the Destination Node parameter. The Select Network Elements form opens.

17 Select a destination NE in the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Destination panel.

18 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

19 Configure the filter criteria. A list of available ports is displayed.

20 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

21 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Action Type
- Continue on individual Failure

22 Click on the Execute button to begin the copy or move operation. The Execution Result panel displays the execution state of the copy or move operation and the number of successful and failed operations based on the input criteria.

Note — When you copy or move a SAP on an L2 interface and there is a non-zero value assigned to the PIM Snooping parameter Maximum Number of Groups, the value is not copied or moved to the new location. You must manually configure the Maximum Number of Groups parameter in the new location.

23 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP copy or move operation. Click on the Refresh button of the Deployments form to update the list, if required.

24 Click on the Result tab button to view a list of the successful and failed operations as identified by the 5620 SAM.

25 Click on the Refresh Result button to view the most recent results.

26 To view the information for an individual SAP copy or move operation, move the mouse pointer over the Message field of the operation.

27 If a copy or move operation fails, you can restore the previous source NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file that was specified in step 2

The SAPs that were deleted during the unsuccessful copy or move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

28 If a copy or move operation partially fails, you can restore the previous destination NE configuration using one of the following methods.

Note — If the copy or move operation fails completely, there is no need to restore the previous configuration because no SAPs are created on the destination NE.

a Restore the backed-up configuration file.

i Open a CLI on the destination NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 4

The previous configuration is restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

b Manually delete the SAPs that the copy or move operation created on the destination NE.

29 Restore the previous automatic configuration backup functionality in the backup policy used by the source NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

30 Restore the previous automatic configuration backup functionality in the backup policy used by the destination NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

31 Close the Copy/Move SAPs and the Deployments forms.

Procedure 20-6 To move L3 access interface SAPs within or between ports on the same NE

Perform this procedure to move one or more L3 access interface SAPs within a port, or from one port to another port on the same NE.

To copy one or more L3 access interface SAPs from one port to another port on the same NE, see Procedure 20-8 for more information.

To copy or move L3 access interface SAPs from one port to another on different NEs, see the *5620 SAM Scripts and Templates Developer Guide* for information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. See chapter 3 for information about using the 5620 SAM clipboard.

Note — L3 access interfaces are not bound to a port; for example, loopback interfaces cannot be moved.

1. For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

2. On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

   admin save *file_name* ↵

   where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

   See the appropriate device documentation for more information about saving the device configuration to a file.

3. Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

   Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP move operation to ensure that faults that may arise during the operation are immediately detected.

   The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the move operation.

4. Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5. Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the Alarm window are all shown.

6. Click on the Result Export Path tab button. The Result Export Path form opens.

7. Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

15 Configure the filter criteria. A list of available ports is displayed.

16 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

17 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

18 Click on the Execute button to start the move operation. The Execution Result panel displays the execution state of the move operation and the number of successful and failed operations based on the input criteria.

19 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

20 Click on the Result tab button to view a list of the successful and failed operations as identified by the 5620 SAM.

21 Click on the Refresh Result button to view the most recent results.

22 To view the information for an individual SAP move operation, move the mouse pointer over the Message field of the operation.

23 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

24 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

25 Close the Copy/Move SAPs and the Deployments forms.

Procedure 20-7 To move L3 subscriber interface SAPs between ports on the same NE

Perform this procedure to move one or more L3 subscriber interface SAPs from one port to another port on the same NE.

To copy or move L3 subscriber interface SAPs from one port to another on different NEs, see the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. However, you can only move all of the SAPs in a group interface; you cannot be used to move a subset of SAPs. See chapter 3 for information about using the 5620 SAM clipboard.

1 For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

2 On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

3 Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP move operation to ensure that any faults that arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the move operation.

4 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5 Arrange the forms on the GUI so that you can view the entire Copy/Move SAPs form, the Deployment form, and the Alarm window.

6 Click on the Result Export Path tab button. The Result Export Path form opens.

7 Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Configure the filter criteria. A list of available ports is displayed.

15 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

16 Configure the parameters:

- Current Mode
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

17 Click on the Execute button to start the move operation. The Execution Result panel displays the state of the move operation, and the number of successful and failed operations based on the input criteria.

18 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

19 Click on the Result tab button to view a list of the successful and failed operations, as identified by the 5620 SAM.

20 Click on the Refresh Result button to view the most recent results.

Note — If one SAP fails, all SAPs under the same group interface fail because the SAPs can only move together. In this case, there is insufficient information to determine which SAP caused the problem using the 5620 SAM.

21 To view information about an individual SAP move operation, move the mouse pointer over the Message field of the operation.

22 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

23 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 23 for more information about configuring automatic configuration backup for an NE.

24 Close the Copy/Move SAPs and the Deployments forms.

Procedure 20-8 To copy L3 access interface SAPs between ports on the same NE

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the L3 Access Interfaces tab button.

5 Choose an L3 access interface and click on the Properties button. The L3 Access Interface (Edit) form opens.

6 Click on the Port tab button.

7 Click on the More Actions button and choose Copy.

   a If you are copying an IES L3 access interface, an L3 Access Interface (Create) form opens. Go to step 9.

   b If you are copying a VPRN L3 access interface, a Select Site form opens. Go to step 8.

8 Select a site and click on the OK button. The L3 Access Interface (Create) form opens.

9 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

10 Click on the Port tab button.

11 Click on the Select button in the Terminating Port panel to choose a port to associate with the L3 access interface. The Select Terminating Port - L3 Access Interface form opens.

12 Configure the filter criteria. A list of available ports appears.

Note — Only ports in access mode appear in the list.

13 Select a port and click on the OK button. The Select Terminating Port - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the port information displayed.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button to confirm the action. The L3 Access Interface (Create) form closes and the service configuration form appears with the newly created L3 access interface.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The service configuration form closes.

Procedure 20-9 To add a queue group to an Ethernet port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a device where an Ethernet port is configured and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and right-click on an Ethernet port. Select Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Ethernet tab button.

6 Perform one of the following:

a Click on the Network Egress Queue Group tab button.

b Click on the Access Egress Queue Group tab button.

c Click on the Access Ingress Queue Group tab button.

Note — The Network Egress Queue Group tab button is available if queue groups are supported on the port, depending on the NE release and IOM type. See section “Port queue groups” in chapter 65 for more information about supported devices and IOM types.

7 Click on the Create button. The Queue Group (Create) form opens with the General tab displayed.

8 Click on the Select button in the Queue Group Template Policy panel. The Select Queue Group Template Policy - Queue Group list form opens.

9 Choose a queue group template policy from the list and click on the OK button. The Select Queue Group Template Policy - Queue Group list form closes.

10 Configure the Description parameter.

11 Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - Queue Group list form opens.

> **Note —** Only the accounting policies with the Type parameter configured to one of the following options are listed:
>
> - Queue Group Octets
> - Queue Group Packets
> - Combined Queue Group

12 Choose an accounting policy from the list and click on the Ok button. The Select Accounting Policy - Queue Group list form closes and the Queue Group (Create) form refreshes with the accounting policy information.

13 Configure the Collect Accounting Statistics parameter.

14 Click on the Select button in the Scheduler Policy panel to assign a scheduler policy to the port. The Select Scheduler Policy - Queue Group list form opens.

15 Choose a scheduler policy from the list and click on the OK button. The Select Scheduler Policy - Queue Group list form closes.

16 If you are adding an access ingress queue group, go to step 23. Otherwise, continue to step 17.

17 Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only if you did not select a scheduler policy in step 15.
The Frame-Based Accounting parameter is configurable only if you configure the Aggregate Rate Limit (kbps) parameter.

18 If you are adding a network egress queue group, go to step 23. Otherwise, continue to step 19.

19 Click on the Host Matching tab button.

20 Click on the Create button. The Host String (Create) form opens.

21 Configure the Host String parameter.

22 Click OK. The Host String (Create) form closes and the information on the Host Matching tab is updated.

23 Click on the Overrides: Queue tab button.

24 Click on the Create button. The Queue Override (Create) form opens.

25 Click on the Select button beside the ID parameter to select an egress queue. The Select Queue - Queue Override list form opens.

26 Choose an entry from the list and click on the OK button. The Select Queue - Queue Override list form closes and the Queue Override (Create) form refreshes with the queue information.

27 Click on the Override Policy Items tab button.

28 Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- PIR (kbps)
- CIR (kbps)

The parameters are configurable when the Override check box is enabled.

29 Click on the OK button to save the configuration and close the Queue Override (Create) form. A dialog box appears.

30 Click on the OK button.

31 Click on the OK button to save the configuration and close the Queue Group (Create) form. A dialog box appears.

32 Click on the OK button. A dialog box appears.

33 Click on the Yes button to save the configuration and close the Physical Port (Edit) form.

34 Close the Network Element (Edit) form.

Procedure 20-10 To configure SONET ports

Perform the steps in this procedure as required depending on the daughter card and port type that you are configuring.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a SONET ports and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Speed
- DDM Event Suppression
- OLC State

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the Channels tab button to configure the SONET/SDH channel.

- **a** Click on the Create button to create a new channel.
- **b** Choose a channel from the list and click on the Properties button to view and edit the channel parameters.
- **c** Choose a channel from the list and click on the Delete button to remove a channel from the port.

9 Click on the SONET tab button.

10 Configure the parameters:

- Framing
- Clock Source
- Loopback
- Single Fiber
- Hold Time Down (100s of ms)
- Hold Time Up (100s of ms)
- Tx DUS/DNU

11 Click on the SONET Monitoring tab button.

12 Configure the parameters:

- BER Signal Degradation Threshold
- BER Signal Failure Threshold
- Report Alarms

13 Click on the SONET Overhead tab button.

14 Configure the parameters:

- SONET Section Trace Mode
- J0 Byte
  Enter a J0 byte that identifies the circuit. This byte is inserted continuously at source. This can be checked against the expected value by the receiver. If no byte is entered, then null is used. The parameter is configurable when the SONET Section Trace Mode is set to Byte.
- J0 String
  The parameter is configurable when the SONET Section Trace Mode is set to String.

15 Click on the other tab buttons in the properties form to view and edit additional port information.

16 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-11 To configure an HSMDA override

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an HSMDA override and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon to the HSMDA card level.

4 Expand the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Override Policy Items tab button. The Override configuration form opens with the HSMDA Scheduler tab displayed.

6 Click on the Create button. The Port Egress HSMDA Scheduler Policy Override (Create) form opens with the General tab displayed.

7 Click on the Override tab button.

8 Configure the parameters:

- Maximum Rate (Mbps)
- Rate (Mbps)
- Weight in Group

The Rate (Mbps) parameter is configurable when a Group is not specified for the applied HSMDA scheduler policy. The Weight in Group parameter is only configurable when Group 1 or Group 2 is specified for the HSMDA scheduler policy.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Override configuration form is updated with the scheduler override.

11 Close the Physical Port (Edit) form.

Procedure 20-12 To configure TDM DS3 ports

Perform the steps in this procedure as required depending on the port type that you are configuring.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a TDM DS3 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the General tab parameters:

- Description
- Speed
- OLC State
- DDM Event Suppression

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the DS3/E3 tab button.

9 Configure the parameters:

- Line Buildout
- Type

10 Click on the other tab buttons in the properties form to view and edit additional port information.

11 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-13 To configure serial ports

Perform this procedure to configure a port on a 12 x Serial Data card on the 7705 SAR.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you need to configure a serial port and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Speed
- Serial Type
- OLC State

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the other tab buttons in the properties form to view and edit additional port information.

9 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-14 To configure a 7210 SAS-M channelized TDM DS1 or E1 port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7210 SAS-M channelized TDM DS1 or E1 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7210 SAS-M port object that contains a channelized DS1 or E1. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- OLC State

6 Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port form opens.

7 Choose an SHG and click on the OK button. The Select Split Horizon Group - Physical Port form closes and the Physical Port (Edit) form refreshes with the SHG name.

Note — To create or delete a 7210 SAS SHG, see Procedure 20-16.

8 Click on the DS1/E1 tab button.

9 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

Note — The Line Impedance parameter only appears when the Port Type parameter is set to E1.

10 Click on the Qos Pool tab button.

11 Choose a QoS pool from the list and click on the Properties button. The QoS Pool (Edit) form opens.

12 Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

13 Choose a slope policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes and the QoS Pool (Edit) form refreshes with the name of the slope policy.

14 Click on the OK button. The QoS Pool (Edit) form closes.

15 Click on the States tab button.

16 Configure the Administrative State parameter.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 20-15 To assign policies to a 7210 SAS Ethernet port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on a 7210 SAS device with a configured Ethernet port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Policies tab button. The Policies form opens with the General tab displayed.

6 Perform one of the following to assign policies to a 7210 SAS Ethernet port.

   a If the port is in access mode, go to step 7.

   b If the port is in network mode or is an L2Uplink port, go to step 8.

7 You can assign port scheduler and access egress policies, and enable queues for statistics collection when the 7210 SAS port mode is access.

   i Click on the 7210 Specific tab button.

   ii Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.

   iii Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.

iv Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.

v Click on the Clear button in the Access Egress Policy panel to remove the selected policy.

vi Click on the Select button in the Access Egress Policy panel to assign an access egress policy to the port. The Select Access Egress Policy - Sas Port form opens.

vii Choose a policy from the list and click on the OK button. The Select Access Egress Policy - Sas Port form closes.

viii If you are configuring the collection of egress packet forwarding statistics, click on the 7210 Statistics tab button. Otherwise, go to step 9.

ix Configure the Queue 1 through Queue 8 parameters, as required.

Note — Enabling these queues is only applicable to the 7210 SAS-E. While any queue of any port can be enabled, only eight counters in total can be enabled for each 7210 SAS-E device.

x Go to step 9.

8 You can assign accounting, port scheduler, network, and network queue policies when the 7210 SAS port mode is network or when it is an L2Uplink port.

i Click on the 7210 Specific tab button.

ii Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.

iii Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.

iv Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.

v Click on the Clear button in the Network Policy panel to remove the selected policy.

vi Click on the Select button in the Network Policy panel to assign a network policy to the port. The Select Network Policy - Sas Port form opens.

vii Choose a policy from the list and click on the OK button. The Select Network Policy - Sas Port form closes.

viii Click on the Clear button in the Network Queue panel to remove the selected policy.

ix Click on the Select button in the Network Queue panel to assign a network queue policy to the port. The Select Network Queue Policy - Physical Port form opens.

x Choose a policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button to apply the changes. The Physical Port (Edit) form closes.

11 Close the Network Element (Edit) form.

Procedure 20-16 To create a 7210 SAS SHG

Traffic that arrives on a access or access uplink port or LAG within an SHG is not copied to other ports and LAGs in the same SHG; the traffic is copied to ports and LAGs in other SHGs if they exist within the same VPLS. Ports and LAGs are added to an SHG when you configure a port or LAG on a 7210 SAS. SHGs are not supported for a VPLS instance.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure the SHG and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Split Horizon Groups tab button.

4 Click on the Create button. The Split Horizon Group (Create) form opens.

5 Configure the parameters:

- Name
- Description

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The SHG is added to the displayed list.

Note 1 — Only one SHG can be configured per service.

Note 2 — A SHG and a Mesh SDP Binding cannot exist simultaneously on a single service.

8 Repeat steps 4 to 7 to add another SHG, if required.

9 To view the ports, LAGs, and faults that are associated with an SHG, choose an SHG from the list and click on the Properties button.

10 If you need to delete an SHG, select the SHG and click on the Delete button. A dialog box appears.

11 Enable the check box and click on the Yes button. You cannot delete an SHG if there are any ports or LAGs bound to it.

12 Close the Network Element (Edit) form.

Procedure 20-17 To configure a 7250 SAS CES TDM DS1/E1 port

Perform this procedure to configure a TDM DS1/E1 port on a CES 2-Port Gig Ethernet MDA card.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7250 SAS CES TDM DS1/E1 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7250 SAS CES port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the T1/E1 tab button.

9 Configure the parameters:

- Line Buildout
- Line Length
- Line Impedance

10 Click on the OK button. A dialog box appears.

11 Click on the OK button.

Procedure 20-18 To configure Telco and 7250 SAS uplink ports as network ports

When you add a 7250 SAS or Telco device to a ring group, the device ports can be used as VLAN service access points or as network uplink ports that receive ring group traffic from a device such as a 7450 ESS.

By default, the Mode parameter for 7250 SAS or Telco devices is set to Access. You can configure the required ports to act as uplink ports by setting the parameter to Network.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure network ports and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Set the Mode parameter to Network.
  An access port is used for customer-facing traffic on which services are configured. The Encap Type parameter for an access port must be set to Dot1 Q.
  A network port participates in the service provider transport or infrastructure network. For 7250 SAS and Telco devices, the network port acts as the uplink for the ring to the transport network. The Encap Type parameter for an uplink port must be set to Dot1 Q.
- Speed
- OLC State

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Configure the other Ethernet port parameters, as described in Procedure 20-1.

Procedure 20-19 To configure a 7705 SAR ASAP channelized TDM port

This procedure applies to 7705 SAR channelized TDM DS1/E1 ports and channelized TDM DS3/E3 ports.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7705 SAR ASAP channelized TDM port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7705 SAR port object that contains a channelized port (DS1/E1 or DS3/E3). The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- OLC State

6 Click on the DS1/E1 or DS3/E3 tab button.

7 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

All ports of the ASAP daughter card are automatically configured to the same port type when the first port is configured. A mix of DS1 and E1 ports or DS3 and E3 ports is not supported. The Port Type parameter can only be modified when no channels are configured on any port of the daughter card. If all of the channels are deleted on the daughter card, the port type is automatically set to DS1 or DS3 for all ports.

8 Click on the States tab button.

9 Configure the Administrative State parameter.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-20 To configure a 7710 SR channelized TDM DS1 or E1 port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a 7710 SR channelized TDM DS1 or E1 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a 7710 SR port object that contains a channelized DS1 or E1. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- OLC State

6 Click on the DS1/E1 tab button.

7 Configure the parameters:

- Port Type
- Line Buildout
- Line Length
- Db Loss

8 Click on the States tab button.

9 Configure the Administrative State parameter.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-21 To configure 9500 MPR Ethernet ports

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure an 9500 MPR Ethernet port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Configure the Port Usage parameter if you are provisioning the following ports:

- ports 1 to 4 on the 2+2 x Ethernet (EAS) card
- ports 5 to 8 on the 4+4 x Ethernet (EAS) card
- ports 1 to 6 on the core-enhanced card

7 Configure the OLC State parameter.

8 Click on the States tab button.

9 Configure the Administrative State parameter.

10 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

11 Configure the parameters:

- Auto-negotiate
- Advertised Capability

Note — Check what combination is supported for Advertised Capability in the *9500 MPR User Guide*.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 20-22 To configure ports on a 2xSTM card for 9500 MPR

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the card where you need to configure the 2xSTM card type and choose Configure card from the contextual menu. The Card Slot (Create) form opens with the General tab displayed.

4 Set the Assigned Card Type parameter to 2xSTM. The card is configured and two ports are displayed.

5 Expand to the port level and right-click on Properties. The Physical Port (Edit) form opens with the General tab displayed.

6 In the Port Usage panel, configure the ports by selecting one of the following:

- EMPTY
- SFP-O
- SFP-E

a When you set the card to SFP-O, the 2xSTM port is configured and the Protection tab is enabled, see Procedure 19-19 in chapter 19 for more information on card Protection. When the card is set to EMPTY, all the configured ports revert back to an empty slot after the port is shutdown.

b When you set the card to SFP-E, the 2xSTM port is configured but the Protection tab is disabled.

c When you set the card to EMPTY, all the configured ports revert back to an empty slot after the port is shutdown.

Note 1 — You need to shut down the configured port to remove the port. Select the port and choose Port→Shut Down. Choose Port→Properties. Configure the Port Usage parameter to EMPTY. The SFP-O ports are removed. You can now configure other ports.

Note 2 — Protection for cards is at the card level. It cannot be configured at the port level. Configure protection for the main cards and the spare cards. Protection is enabled only for the SFP-O port.

Note 3 — 1+1 Protection can be set at different card levels. This provides redundancy. Both cards should be enabled and configured to SFP-O before protection is set.

7 After the SFP-O ports are configured, choose Card→Properties. The Card [Edit] form is displayed with the Protection tab enabled.

8 Set the Protection Type parameter to 1+1 EPS protection. All of the SFP-O ports are protected.

9 Click on the OK button to save the change. A dialog box appears.

10 Click on the Yes button. The Card [Edit] form closes.

Procedure 20-23 To configure a port on a 1xSTM Channelized card for 9500 MPR

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the card where you need to configure the 1xSTM Channelized card type and choose Configure card from the contextual menu. The Card Slot [Create] form opens with the General tab displayed.

4 Set the Assigned Card Type parameter to 1xSTM (Channelized).

5 Expand to the port level and right-click on Properties. The Physical Port [Edit] form opens with the General tab displayed.

6 In the Port Usage panel configure the port by selecting one of the following:

- EMPTY
- SFP-O
- SFP-E

a When you set the card to SFP-O, the 1xSTM Channelized port is configured, 63E1 channels are created. You can enable the E1 channel, see Procedure 20-24 for more information. The Protection tab is enabled, see Procedure 19-19 in chapter 19 for more information on card Protection. If the card is set to EMPTY, the configured port reverts back to an empty slot after the port is shutdown.

b When you set the card to SFP-E, the 1xSTM Channelized port is configured, 63E1 channels are created, but the Protection tab is disabled.

c When you set the card to EMPTY, the configured port reverts back to an empty slot after the port is shutdown.

Note 1 — You need to shut down the configured port to remove the port. Select the port and choose Port→Shut Down. Choose Port→Properties. Configure the Port Usage parameter to EMPTY. The SFP-O ports are removed. You can now configure other ports.

Note 2 — Protection for cards is at the card level. It cannot be configured at the port level. Configure protection for the main cards and the spare cards. Protection is enabled only for the SFP-O port.

Note 3 — 1+1 Protection can be set at different card levels. This provides redundancy. Both cards should be enabled and configured to SFP-O before protection is set.

7 Once the SFP-O port is configured, select Card→Properties. The Card [Edit] form is displayed with the Protection tab enabled.

8 From the Protection Type drop down menu, select 1+1 EPS protection. The SFP-O port is protected.

9 Click on the OK button to save the change. A dialog box appears.

10 Click on the Yes button. The Card [Edit] form closes.

Procedure 20-24 To configure 9500 MPR E1 and DS1 ports

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure a 9500 MPR E1 or DS1 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Configure the OLC State parameter.

7 Click on the States tab button.

8 Configure the Administrative State parameter.

9 Click on the DS1/E1 tab button.

10 Configure the parameters:

- Signal Mode
- Line Code
- Line Code

If you are configuring an E1 port you can only configure the Signal Mode parameter.

11 Click on the other tab buttons in the properties form to view additional port information.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 20-25 To configure 9500 MPR DS3 ports

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand the 9500 MPR NEs icon.
3. Right-click on the device where you want to configure a 9500 MPR DS3 port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.
4. On the Network Element (Edit) form navigation tree, expand the Shelf icon.
5. Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.
6. Configure the OLC State parameter.
7. Click on the States tab button.
8. Configure the Administrative State parameter.
9. Click on the DS3/E3 tab button.
10. Configure the parameters:
    - Signal Mode
    - Line Code
    - AIS Signal Type
11. Click on the other tab buttons in the properties form to view additional port information.
12. Click on the OK button. A dialog box appears.
13. Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 20-26 To manage 9500 MPR radio modem ports

Note — The 5620 SAM supports limited configuration of radio modem ports on the 9500 MPR.

You can configure MPT radio ports for SFP, MPT-HC, MPT-HCv2, MPT-MC, MPT-HL, or MPT-ACC depending on the card type that is installed in the 9500 MPR device.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand the 9500 MPR NEs icon.

3 Right-click on the device where you need to configure a 9500 MPR radio modem port and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and select a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Configure the Port Usage parameter if you are provisioning the following ports:

- ports 1 to 4 on the 2+2 x Ethernet (EAS) card
- ports 5 to 8 on the 4+4 x Ethernet (EAS) card
- ports 1 to 6 on the core-enhanced card

7 Configure the OLC State parameter.

8 Click on the Radio tab button to view radio modem port parameters.

9 Click on the other tab buttons in the properties form to view additional port information, such as physical links and statistics.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 20-27 To configure 9500 MPR port segregation

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure port segregation and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on a shelf object. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Port Segregation tab button.

6 Click on the Add button.

7 The Add Member Wizard form appears with the From Port step displayed.

8 Click on the Select button beside the From Port field. The Select From Port - Port Segregation form opens.

9 Select a port from the list.

10 Click on the OK button. The Select From Port - Port Segregation form closes. and the Add Member Wizard form reappears.

11 Click on the Next button. The To Port step is displayed.

12 Choose a port from the list and click on the Finish button.

13 A dialog box appears. Click on the OK button. The Add Member Wizard form closes.

14 Perform one of the following.

  a To add more port combinations, repeat steps 6 to 13.

  b Go to step 15.

15 Click on the OK button. The Shelf (Edit) form closes.

Procedure 20-28 To configure analog performance management on 9500 MPR radio modem ports

This procedure provides the analog radio statistics for 9500 MPR radio modem ports.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure analog performance management and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Statistics tab button.

7 In the Select Object Type area, choose Radio Analog Statistics (Radio Equipment) from the contextual menu.

8 Click on the Collect button.

9 A statistics record appears on the Physical Port (Edit) form. Select the record.

10 Click on the Properties button. The Statistics Record - Radio Analog Statistics form opens.

11 View the read-only analog performance parameter values for the radio modem port.

12 Click on the Close button. The Statistics Record - Radio Analog Statistics form closes.

13 Close the Physical Port (Edit) form.

Procedure 20-29 To configure power source type on 2+2 x Ethernet (EAS) card slots for 9500 MPR

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure a power source type and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the card level and click on a 2+2 x Ethernet (EAS) card slot object. The Card Slot (Edit) form opens with the General tab displayed.

6 Click on the Power Source tab button.

7 Select a displayed interface or click on the Search button if no interface is displayed, then select a displayed interface. The Power Source (edit) form opens.

8 In the Power Source panel, configure the Type parameter.

9 Click the OK button. The Power Source (Edit) form closes.

10 The Card Slot (Edit) form reappears. Click on the OK button. A dialog box appears. Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 20-30 To configure power level performance management on 9500 MPR radio modem ports

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure power level performance management and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Statistics tab button.

7 In the Select Object Type area choose one of the following from the contextual menu:

- Hop Current Data Stats
- Link Current Data Stats
- RSL Hop Current Data Stats
- TSL Hop Current Data Stats

8 Click on the Collect button.

9 A statistics record appears on the Physical Port (Edit) form. Select the record.

10 Click on the Properties button. The Statistics Record - RSL/TSL Hop Current Data Stats form opens.

11 View the read-only power level performance parameter values for the radio modem port.

12 Click on the Close button. The Statistics Record - Radio Analog Statistics form closes.

13 Close the Physical Port (Edit) form.

Procedure 20-31 To add 9500 MPR port protection

Note 1 — The Protection tab button only appears for MPT-type ports of EAS modules if the corresponding spare port has been configured as MPT.

Note 2 — All cross connections, flow-ids, and sync sources must be removed from the port under the spare card slot before protection can be enabled.

Note 3 — To configure protection type 1+1 FD on MPT/Radio, the Mode cannot be Adaptive Modulation.

Note 4 — In Release 3.0.0, for the 2+2 EAS MPT ports, the protect port can be chosen as either the consecutive port of the same card or the same port of the corresponding even slot.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR icon, right-click on the 9500 MPR object you need to configure as the main port of the protection pair and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Card Slot icon and click on the port object that you need to configure. The Port (Edit) form opens with the General tab displayed.

5 Click on the Protection tab button.

6 Configure the Protection Type parameter on the main/spare MPT port.

7 For radio ports, configure the parameters:

- Restoration Criteria in the Receiver Protection Scheme Parameters panel
- Commands Receiver Protection Scheme Parameters panel
- Restoration Criteria in the Transmitter Protection Scheme Parameters panel.
- Commands in the Transmitter Protection Scheme Parameters panel.

Note — For Protection Type 1+1 FD, Transmitter Protection Scheme parameters are not applicable.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Port (Edit) form closes.

10 Verify that the protection has been enabled. The status of the main port should be Active and the status of the spare port should be Standby.

Procedure 20-32 To remove 9500 MPR port protection

Note — If 1+1 HSB is configured as the protection type for an MPT port, the transmitter must be muted from the NEtO to remove the protection.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR icon, right-click on the 9500 MPR spare port object and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand the Card Slot icon and click on the port object that you need to configure. The Port (Edit) form opens with the General tab displayed.

5 Click on the Protection tab button.

6 Set the Protection Type parameter to No Protection.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Port (Edit) form closes.

9 Verify that the protection has been removed from the previously main and spare ports.

Procedure 20-33 To configure a loopback test on a 9500 MPR DS1, ES1 or radio modem port

Perform the steps in this procedure as required on the port type that you are configuring.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 9500 MPR NEs icon.

3 Right-click on the device where you want to configure a loopback test and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a 9500 MPR port object (DS1, ES1, or radio modem). The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Loopback tab button.

7 Select an interface. Click on the Properties button.

8 The Loopback (Edit) form opens.

9 Configure the parameters:

- Activation
- Timeout Period (Days)
- Timeout Period (Hrs)
- Timeout Period (Mins)

10 Click on the OK button. The Loopback (Edit) form closes.

11 On the Physical Port (Edit) form, click on the OK button.

12 The Physical Port (Edit) form closes.

Note — If the card containing the ports is not equipped but configured, a loopback test cannot be performed on the physical ports of the card.

Procedure 20-34 To configure OmniSwitch Ethernet ports

Perform the steps in this procedure as required depending on the OmniSwitch chassis type and port type that you are configuring. Different chassis types display different port configuration parameters.

Note — You can configure MVRP fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device for which you need to configure an OmniSwitch Ethernet port and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- Mode

  An access port is used for customer-facing traffic on which VLAN services are configured.

  A network port or channel is configured for network access in the service provider transport or infrastructure network. Typically, only one OmniSwitch network port is required for tree topology, and two ports are required for ring topology.
- Speed
- MTU (bytes)
- Automatic VLAN Binding
- OLC State

6 Click on the States tab button.

7 Configure the Administrative State parameter.

8 Click on the Policies tab button.

Note — A port must have a service access point associated with it before you can apply a UNI policy to the port.

9 Click on the Select button in the UNI Profile panel to assign a UNI policy to the port. The Select UNI Profile - Physical Port form opens.

10 Choose a User Network Interface (UNI) profile policy from the list and click on the OK button. The Select UNI Policy - Physical Port form closes.

11 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

12 Perform one of the following:

a For OS 6900 and OS 10K devices, configure the following parameters:

- Duplex
- Enable Broadcast Limit Mode
- Broadcast Limit
- Enable Multicast Limit Mode
- Multicast Limit
- Enable Unknown Unicast Limit Mode
- Unknown Unicast Limit
- Type

b For all other OmniSwitch devices, configure the following parameters:

- Duplex
- Auto-negotiate
- Enable Port Mobility
- Dot1 Q Acceptable Frames
- Broadcast Limit (kbps)
- Enable Multicast Limit Mode
- Inter-Frame Gap (bytes)
- Detection
- Default VLAN Restore
- Default VLAN Enable
- Ignore BPDU
- Authenticate
- Ingress Filtering

The Inter-Frame Gap (bytes) parameter is only configurable on Gigabit Ethernet ports.

The Default VLAN Restore, Default VLAN Enable, Ignore BPDU, Authenticate, and Ingress Filtering parameters are only configurable when the Enable Port Mobility parameter is set to Enable.

13 Click on the LLDP tab button, if required. The LLDP configuration form opens with the Nearest Bridge tab displayed.

14 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs

15 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers that are associated with the port. The remote peers are used to determine the physical topology of the network.

16 Click on the MVRP tab button to configure MVRP, if required.

17 Configure the parameters on the General tab:

- Status
- Registration Mode
- Applicant Mode
- Periodic Transmission Status
- Join Timer
- Leave Timer
- Leave All Timer
- Periodic Timer

18 Click on the VLAN Restrictions tab button to configure VLAN restrictions, if required:

i Click on the Create button. The MVRP VLAN Registration form appears.

ii Configure the parameters:

- VLAN
- Restrict-Static-VLAN-Registration
- Restrict-Registration
- Restrict-Advertisement

iii Click on OK to close the MVRP VLAN Registration form. The list on the VLAN Restrictions tab is updated with the new MVRP VLAN Registration entry.

19 Click on the QoS tab button, if required. The QoS configuration form opens with the General tab displayed.

20 Configure the parameters:

- QoS Status
- Trusted
- Default 802.1p
- Default DSCP
- Max Egress BW (kbps)
- Max Ingress BW (kbps)
- Servicing Mode
- Default Classification

21 Click on the Queue tab button.

22 If you specified WRR or DRR for the Servicing Mode parameter, configure the Q0 to Q7 parameters in the Weight panel.

23 Configure the Q0 to Q7 parameters in the Minimum Bandwidth (Kbps) panel.

24 Configure the Q0 to Q7 parameters in the Maximum Bandwidth (Kbps) panel.

25 Click on the DHCP Snooping tab button, if required. The tab is only available when the port is associated with a VLAN that has DHCP snooping enabled or DHCP snooping is enabled at the switch level.

26 Configure the parameters:

- Trust Mode
- IP Source Filtering

27 Click on the Ethernet Hybrid tab button, if required. The tab is only available for hybrid Ethernet ports.

28 Configure the parameters:

- Mode
- Speed
- Duplex
- Auto-negotiate
- Detection

29 Click on the PoE tab button, if required. The tab is only available for PoE ports.

30 Configure the parameters:

- Power State
- Maximum Power (milliwatt)
- Power Priority

31 Click on the LPS Learned MAC Entries tab button to view the MAC addresses learned on the port. LPS must be enabled on the port. See Procedure 31-54 for linformation about configuring LPS on an Ethernet port.

32 Click on the Create button to add static MAC address entries, if required. The MAC Entries (Create) form opens.

Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses to the port.

33 Click on the Select button. The Select VLAN Site - MAC Entries form opens.

34 Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

35 Choose a VLAN from the list.

36 Click on the OK button. The Select VLAN Site - MAC Entries form closes.

37 Configure the MAC Address parameter and click on the Apply button to save the changes

38 Repeat steps 32 to 37 to add another MAC address, if required.

39 Click on the OK button. A dialog box appears.

40 Click on the Yes button. The Select VLAN Site - MAC Entries form closes.

41 Click on the OK button. The Physical Port (Edit) form closes.

20.7 Channel and framing link configuration procedures

Use the following procedures to manage channels and framing links using the navigation tree.

Procedure 20-35 To configure SONET clear channels

Perform this procedure to configure SONET clear channels on OC3 to OC192 ports that provide clear channel services. Each port supports one clear channel.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a clear channel port and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a clear channel port object. The Physical Port (Edit) form opens with the General tab displayed. SONET is the default framing scheme.

Note — A clear channel port is a port on a card that is not designated Deep Channelized.

5 Configure the parameters:

- Description
- Speed

6 Click on the Apply button.

7 In the navigation tree, right-click on the port and choose Create Channel. The Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

8 Configure the parameters:

- Description
- Configured MAC
- Mode
- Encap Type
- MTU (bytes)
- DDM Event Suppression
- Load Balance Algorithm

The Encap Type parameter is configurable when the Mode parameter is set to Access.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

9 Click on the Apply button to save the changes. The STS*n* clear channel appears in the navigation tree under the port of the daughter card.

a If the Encap Type parameter of the port is ATM, the form is refreshed.

b If the Encap Type parameter of the port is not ATM, go to step 14.

10 Click on the More Actions button and choose Edit ATM to configure the ATM interface. The ATM interface form opens with the General tab displayed.

11 Configure the parameters:

- ATM Interface Cell Format
- ATM Minimum VPI Value
- Interface Mapping

12 To create an ILMI link, see Procedure 20-48.

13 Click on the OK button. The ATM Interface form closes.

14 Close the Channel (Edit) form.

Procedure 20-36 To perform a bulk channel creation on ports for card types that support multiple sub-channels

Perform this procedure to create the maximum number of channels on ports for card types that support multiple sub-channels. Table 20-5 lists the nodes and cards that support bulk channel creation.

Table 20-5 Node and cards that support bulk channel creation

Node	OC3	OC12	DS3 ASP	E3 ASP
7450 ESS	X	X	X	X
7705 SAR-M	X	—	—	—
7710 SR	X	X	X	X
7750 MG	X	X	X	X

Note — This procedure assumes you have pre-configured a node with an appropriate daughter card that supports multiple sub-channels.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate and expand the device on which you need to perform a bulk channel creation.

3 Right-click on a port object and choose Create Maximum Number Of Channels from the contextual menu. The Create Maximum Number Of Channels form opens.

4 Configure the parameters, as required:

- Channel Type
- STs1 Channel Payload Type
- Ds3 Channel Payload Type
- Vt15 Channel Payload Type
- Time Slots per DS0 Channel Group
- Encap Type

5 Click on the Execute button. The channels and sub-channels appear in the navigation tree under the port of the daughter card.

Procedure 20-37 To configure SONET sub-channels

SONET sub-channels are available on deep channelized OC12 and OC3 ports. SONET STS1 channels support the following payload types:

- DS3
- VT15
- VT2

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure SONET sub-channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level, right-click on a port object and choose Create Channel. The Create Channel form opens with the General tab displayed.

Note — When there are no channels available on that port, the Create Channel menu option menu is dimmed

5 Configure the parameters:

- Local Channel ID
  - For an OC3 port, use a value from 1 to 3.
  - For an OC12 port, use a value in the format <1 to 4>.<1 to 3>
- Payload Type
- DDM Event Suppression

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

6 Click on the Apply button.

The STS1 (AU3) channel appears in the navigation tree under the port of the daughter card.

7 Create the STS1 (AU3) sub-channels according to the payload type configured:

a To create VT15 (Sdh TU11) sub-channels, go to Procedure 20-39.

b To create VT2 (Sdh TU12) sub-channels, go to Procedure 20-39.

c To create a DS3 or E3 (SDH framing only) clear channel, go to step 8.

8 To create a DS3 or E3 clear channel, perform the following steps:

i From the navigation tree, select an STS1 or AU3 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens.

- For AU3 channels, DS3 and E3 channelization is available.
- For STS1 channels, only DS3 channelization is available.

ii Configure the Description parameter.

iii Configure the Channelized parameter.

- Choose Ds1 to channelize the DS3 to carry up to 28 DS1 channelized to the DS0 level.
- Choose E1 to channelize the DS3 to carry up to 21 E1 channelized to the DS0 level.
- Choose None to create a DS3 or E3 clear channel. Configure the following parameters:
  - Configured MAC
  - Encap Type
  - Speed
  - MTU (bytes)
  - Load Balance Algorithm

iv Click on the OK button.

If you set the Channelized parameter to None, a DS3 clear channel in Access mode is created under the STS1 or the AU3 in the navigation tree.

If you set the Channelized parameter to DS1, a DS3 channelized for DS1 is created under the STS1 (AU3). Go to step 11 in Procedure 20-43 to create the DS1 channels.

If you set the Channelized parameter to E1, a DS3 channelized for E1 is created under the STS1 (AU3) in the navigation tree. Go to step 11 in Procedure 20-43 to create the E1 channels.

Procedure 20-38 To configure SDH sub-channels

SDH sub-channels are available on deep channelized OC12 and OC3 ports. SDH AU4 channels support the following payload types:

- TU3
- TU11
- TU12

SDH AU3 channels support the following payload types:

- DS3
- E3
- TU11
- TU12

Perform this procedure to configure SDH sub-channels on ports that provide channelized services. You must first configure port framing to SDH since default framing on SONET/SDH ports is SONET.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure SDH sub-channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a deep channelized port. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the SONET tab button and set the Framing parameter to SDH.

6 Click on the OK button.

7 Right-click on the port again and choose Create Channel from the contextual menu. The Channel Type Selection window opens.

8 Choose one of the following channel types and click on the OK button:

a SONET Sts1 (Sdh Au3).

SONET STS1 channelization and SDH AU3 channelization are equivalent. Go to step 5 of Procedure 20-37.

b SONET Sts3 (Sdh Stm1).

The Sts3 SONET Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

The Payload Type parameter for SDH STM1 (AU4) is set to TUG3. There is no SONET framing equivalent. Go to step 9.

9 Configure the parameters:

- Description
- Local Channel ID

10 Click on the States tab button.

11 Configure the Administrative State

12 Click on the OK button. The STM1 (AU4) channel appears in the navigation tree under the port of the daughter card. It contains three TUG3 groups.

13 Right-click on a TUG3 group and choose Properties from the contextual menu. The Sdh Tug3 (Edit) form opens with the General tab displayed.

14 Choose one of the following options to configure the Payload Type parameter:

a PDH Tu3. Click on the Cancel button and go to step 15 to create a TU3 channel.

b SONET VT15 (SDH Tu11). Click on the Apply button and go to Procedure 20-39.

c SONET VT2 (SDH Tu12). Click on the Apply button and go to Procedure 20-39.

15 To create a TU channel, right-click on the TUG3 group and choose Create Channel from the contextual menu. The TU3 Channel (Create) form opens.

16 Configure the parameters:

- Description
- Payload Type

17 Click on the States tab button.

18 Configure the Administrative State

19 Click on the OK button. A TU3 channel is created under the TUG3 group in the navigation tree.

20 Right-click on the Tu3 and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

The E3 is the only payload type available.

21 Configure the parameters:

- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

22 Click on the States tab button.

23 Configure the Administrative State

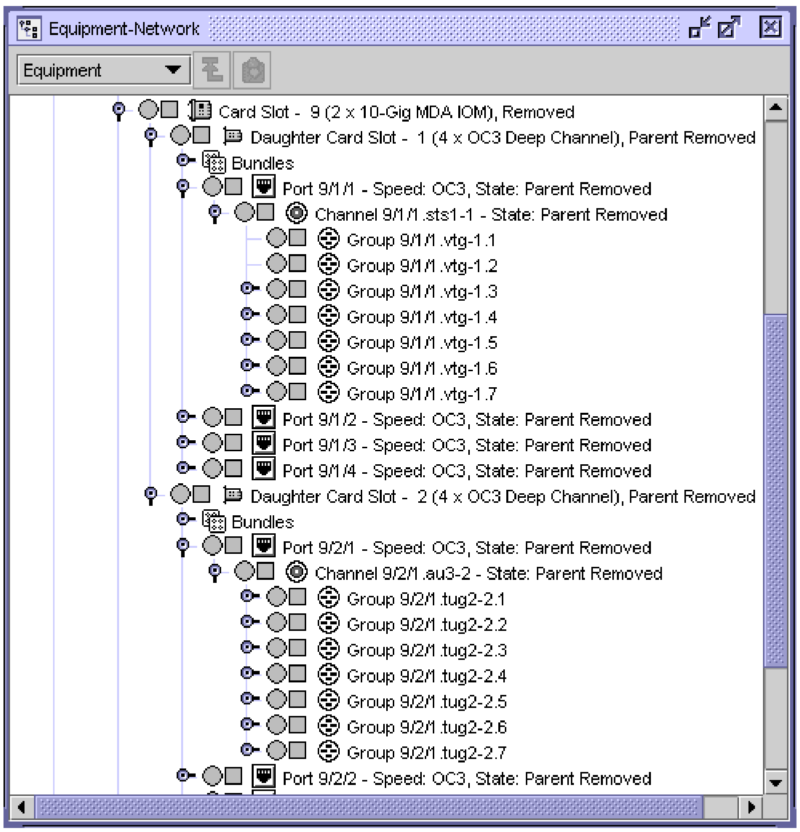
24 Click on the OK button. An E3 clear channel is created under the AU4/TUG3 in the navigation tree.

Procedure 20-39 To create VT15 (TU11) or VT2 (TU12) sub-channels

A SONET VTG and an SDH TUG2 are equivalent groups. A VTG contains four VT15 channels or three VT2. A TUG2 contains four TU11 channels or three TU12. An SDH TUG 3 has no SONET equivalent, however, it contains seven TUG2. (An STM1/AU4 contains three TUG3). See “Comparison of SONET and SDH hierarchies” in section 20.3.

An STS1 channelized to carry a VT15 or VT2 payload type contains seven VTG. An AU3 or a TUG3 channelized to carry a TU11 or TU12 payload type contain seven TUG2. STS1 and AU3 channelization are shown in Figure 20-11.

Figure 20-11 SONET VTG and SDH TUG2 in navigation tree



Each VTG (TUG2) supports up to four VT15 (TU11) channels or three VT2 (TU12) channels. Create each VTG/TUG2 channel one at time.

1 Complete Procedure 20-37 or Procedure 20-38 to carry a VT15 (TU11) or VT2 (TU12) payload type.

  a Go to step 2 to create a VT15 (TU11) channel.

  b Go to step 3 to create a VT2 (TU12) channel.

2 To create a VT15 (TU11) channel, perform the following steps:

  i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

  ii Right-click on the device where you want to create a VT15 (TU11) channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

  iii On the Network Element (Edit) form navigation tree, expand the Shelf icon.

  iv Expand to the channel level, right-click on a VTG or TUG2 channel group that is to carry a VT15 (TU11) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

  v Configure the parameters:

  - Local Channel ID

    Set the Local Channel ID to a value in the range 1 to 4 since there are four VT15 (TU11) in a VTG (TU2).
  - Description

  The default payload type for a VT15 (TU11) channel is PDH DS1. There is no other available payload type.

  vi Click on the OK button. A VT15 channel is created under the VTG or a TU11 channel is created under the TUG2 in the navigation tree.

  vii Right-click on a VT15 or TU11 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

  The Local Channel ID is equal to the VT15 channel Local Channel ID parameter and the channel type is set to DS1 since a VT15 or TU11 channel supports one DS1.

  viii Click on the OK button A DS1 channel is created under the VT15 or the TU11 in the navigation tree.

  You can create up to 28 VT15 (TU11) channels on a VTG (TUG2).

ix Repeat steps 1 and 2 for each VT15 (TU11) channel that you want to create.

x Since a DS1 channel is not used as a SAP, create a DS0 group for each DS1 channel created. Go to step 12 of Procedure 20-43.

3 To create a VT2/TU12 channel, complete these steps:

i From the navigation tree, select a VTG or TUG2 channel group to carry a VT2 (TU12) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

ii Configure the parameters:

- Local Channel ID
  Set the Local Channel ID to a value in the range 1 to 3 since there are three VT2 (TU12) in a VTG (TUG2).
- Description
- Payload Type
  PDH E1 is not available for SONET framing.

iii Click on the OK button. A VT2 channel is created under the VTG, or a TU12 channel is created under the TUG2 in the navigation tree.

iv Right-click on the VT2 or TU12 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

The Local Channel ID is equal to the VT2 channel Local Channel ID parameter, since a VT2 channel supports one E1 or DS1.

v Click on the States tab button.

vi Configure the Administrative State parameter.

vii Click on the OK button. A DS1 channel is created under the VT2 in the navigation tree. An E1 or DS1 is created under the TU12. You can create up to 21 VT2 (TU12) channels on a VTG (TUG2).

viii Repeat steps 1 and 2 for each VT2 (TU12) that you want to create.

ix Since a DS1/E1 channel is not used as a SAP, create a DS0 group for each DS1 or E1 channel created. Go to step 12 of Procedure 20-43.

Procedure 20-40 To create TDM DS1 channels

Perform this procedure to create DS1 channel and children objects from a channelized DS1 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure TDM DS1 channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- OLC State

6 Select the DS1/E1 tab and configure the parameters:

- Port Type
- Line Length

7 Click on the OK button.

8 Right-click on the port again and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

9 Click on the OK button.

10 To create DS0 channel groups, complete these steps:

i From the navigation tree, select a DS1 or E1 channel and choose Create Channel from the contextual menu. The DS0 Channel Group (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID
  For a DS0 group from a DS1 choose from 1 to 24. For a DS0 group from an E1, choose from 2 to 32.
- Description
- Mode
- Encap Type
- MTU (bytes)

Note 1 — All channel groups on a 7705 SAR ASAP port must have the same mode configured. When the first channel group is configured, all other channel groups on the port must be set to the same mode.

Note 2 — The default encapsulation type for the 7705 SAR is N/A. The encapsulation type must be changed from N/A to a valid type. After a valid encapsulation type is configured for a channel group, the encapsulation type cannot be changed for that channel group. To change the encapsulation type, the channel group must be deleted and recreated.

Note 3 — On a 16/32x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 19-24 for more information on configuring the MDA mode.

iii Click on the Channel Group tab button.

iv Configure the parameters:

- CRC Precision
- Scramble
- Idle Cycle Flags
- Time Slots

  Choose one or more timeslots. You can use the Select All and Deselect All buttons.

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 20-41 To configure TDM DS1 or E1 channels

Perform this procedure to edit properties of a DS1/E1 channel and children objects from a channelized DS1/E1 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure TDM DS1 or E1 channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a DS1 or E1 channel. The DS1/E1 Channel (Edit) form opens with the General tab displayed.

5 Click on the States tab button.

6 Configure the Administrative State parameter.

7 Add a DS0 channel group, if required. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Create Cha... tab button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Mode
- Encap Type
- Speed
- MTU (bytes)

Note — On a 16/32x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 19-24 for more information on configuring the MDA mode.

iv Click on the OK button. The DS0 Channel Group (Create) form closes and a dialog box appears.

v Click on the OK button.

8 Click on the Channel tab button.

9 Configure the parameters:

- Channel Framing
- Clock Source
- Loopback
- Report Alarms
- Respond to Remote Loop Signal
- Signal Mode

10 Click on the Statistics tab button to view statistical information.

11 Click on the Faults tab button to view alarm information.

Note — If are configuring a 7705 SAR and selected a clock source of adaptive, you can click on the Adaptive Clock History tab button to view channel adaptive clock performance data for the preceding 15 minutes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The DS1/E1 Channel (Edit) form closes.

Procedure 20-42 To create serial channels

Perform this procedure to create serial channel and child objects from a Serial Data Interface port.

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2. Right-click on the device where you want to configure serial channels and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3. On the Network Element (Edit) form navigation tree, expand to the port level.

4. Right-click on the port and choose Create Channel from the contextual menu. The Serial Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

5. Click on the States tab button.

6. Configure the Administrative State parameter.

7. Click on the Apply button. The Serial Channel (Edit) form refreshes with additional tabs.

8. Click on the Channel tab button.

9. Configure the parameters:

    - Device Mode
    - Gender
    - Speed
    - Loopback
    - Multidrop Data Bridge
    - S-Bit Signalling
    - HCM Data Position
    - Character Length
    - Parity
    - Stop Bits
    - Report Alarms
    - DTR / DSR Input
    - RTS / DCD / C / I Input
    - ALB / CTS Input
    - RDL / RI Input
    - DSR / DTR Output
    - DCD / RTS / I / C Output
    - CTS / ALB Output
    - RI / RDL Output

    Depending on the serial type of the configured port, different parameters are configurable in the Control Leads panel.

10. Create DS0 channel groups:

    i. Click on the SubChannels tab button.

    ii. Click on the Create Cha... button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Description
- Encap Type
- MTU (bytes)

Note 1 — The default encapsulation type for the 7705 SAR is N/A. The encapsulation type must be changed from N/A to a valid type. After a valid encapsulation type is configured for a channel group, the encapsulation type cannot be changed for the channel group. To change the encapsulation type, the channel group must be deleted and re-created.

Note 2 — On an SDI MDA, you must configure the serial type to X.21 or V.35 to use the FR encapsulation type. See Procedure 20-13 for more information.

iv Click on the OK button. The DS0 Channel Group (Create) form closes.

11 Close the Serial Channel (Edit) form.

Procedure 20-43 To create TDM DS3 channels

Perform this procedure to create DS3 channel and children objects from a channelized DS3 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create a TDM DS3 channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port. The Physical Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Description
- OLC State

6 Choose the DS3/E3 tab and configure the parameters:

- Line Buildout
- Type. Choose DS3.

7 Click on the OK button.

8 Right-click on the port again and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

9 To configure the DS3/E3 channel, complete these steps:

a Configure the Channelized parameter to DS1 or E1, if you want to channelize to the DS0 level.

b Configure the Channelized parameter to None if this is a clear channel application.

Configure the parameters as required:

- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

The Local Channel ID parameter is configured automatically and the mode is always Access for TDM.

Note — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 19-24 for more information on configuring the MDA mode.

10 Click on the OK button.

If this is a Channelized DS1 or E1 application, continue to step 11.

11 To create Ds1 or E1 channels, complete these steps:

i From the navigation tree, select a Ds3 channel and choose Create Channel from the contextual menu. The Create DS1/E1 Channel form opens.

ii Configure the Local Channel ID parameter.

- For DS1 choose from 1 to 28.
- For E1 choose from 1 to 21.

iii Click on the OK button. The DS1 or E1 channels are created under the DS3 in the navigation tree.

12 To create DS0 channel groups, complete these steps:

i From the navigation tree, select a DS1 or E1 channel and choose Create Channel from the contextual menu to create DS0 groups. The DS0 Channel (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID
  For a DS0 group from a DS1 choose from 1 to 24. For a DS0 group from an E1, choose from 2 to 32.
- Description
- Configured MAC
- Mode
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

Note — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 19-24 for more information on configuring the MDA mode.

iii Click on the Channel Group tab button.

iv Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots
  Choose one or more timeslots. You can use the Select All and Deselect All buttons.
- BER SF Link Down

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 20-44 To configure TDM DS3 channels

Perform this procedure to edit properties of a DS3 channel and children objects from a channelized DS3 port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure TDM DS3 channels and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a DS3 channel. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the Channelized parameter and click on the Apply button.

a If you choose None, go to step 7.

b If you choose DS1 or E1, perform steps 12 to 35.

7 Configure the parameters:

- Configured MAC
- Speed
- MTU (bytes)
- Load Balance Algorithm

8 Configure the Encap Type parameter and click on the Apply button.

a If you choose BCP Null, BCP DOT1 Q, or IPCP, go to step 9.

b If you choose FR, go to step 10.

c If you choose Cisco HDLC, go to step 11.

d If you choose WAN Mirror, perform steps 13 to 22.

9 Configure the PPP interface for the channel, if required. Perform the following steps:

i Click on the More Actions button and choose Edit PPP. The PPP Interface form opens with the General tab displayed.

ii Configure the parameters:

- Period
- Drop Count

iii To view port, PPP control protocol, statistics, or alarm information for the PPP interface, click on the appropriate tab button.

iv Click on the OK button. The PPP Interface form closes.

v Perform steps 13 to 22.

10 Configure the FR interface, if required. Perform the following steps:

i Click on the More Actions button and choose Edit FR. The FR Interface form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Link Identifier
- Error Threshold
- Monitored Events
- Polling Interval
- Full Enquiry Interval

iii Click on the Frf12 tab button.

iv Set the Mode parameter to Enabled.

v Configure the Fragment Threshold parameter.

vi Click on the Select button beside the MCFR Egress QoS Profile parameter. The Select MCFR Egress Qos Profile - FR Configuration form opens.

vii Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - FR Configuration form closes and the FR Interface form is refreshed with the MCFR Egress QoS Profile information.

viii To view port, statistical, or alarm information for the FR interface, click on the appropriate tab button.

ix Click on the OK button. The FR Interface form closes.

x Perform steps 13 to 22.

11 Configure the Cisco HDLC information.

i Click on the Cisco HDLC tab button.

ii Configure the parameters:

- Keep Alive (seconds)
- Up Count
- Down Count

iii Perform steps 13 to 22.

12 Configure the DS1 and DS0 channels. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Create button. The DS1/E1 Channel (Create) form opens with the General tab displayed.

iii Configure the Local Channel ID parameter.

iv Click on the States tab button.

v Configure the Administrative State parameter.

vi Click on the OK button. The DS1/E1 Channel (Create) form closes.

13 Click on the States tab button.

14 Configure the Administrative State parameter.

15 Click on the Channel tab button.

16 Configure the parameters:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Subrate Range
- Loop Respond
- Report Alarms
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

17 Click on the Message Data Link tab button.

18 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 20-6 describes the MDL message options.

Table 20-6 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

19 Click on the Terminations tab button to view channel termination information.

20 Click on the Statistics tab button to view statistical information.

21 Click on the Faults tab button to view alarm information.

22 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

23 Right-click on a DS1 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

24 Click on the States tab button.

25 Configure the Administrative State parameter, if required.

26 Add a DS0 channel group, if required. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Create button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

Note — On a 4x Channelized ASAP, you must configure the MDA mode in order to use certain encapsulation types. See Procedure 19-24 for more information on configuring the MDA mode.

iv Click on the OK button. The DS0 Channel Group (Create) form closes.

27 Click on the Channel tab button.

28 Configure the parameters:

- Channel Framing
- Clock Source
- Idle Cycle Flags
- Loopback
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

29 Click on the Statistics tab button to view statistical information.

30 Click on the Faults tab button to view information about alarms.

31 Click on the OK button. The channel properties form closes.

32 Configure timeslots for the DS0 channel group. Perform the following steps.

i Choose a DS0 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

ii Configure the parameters, as required.

iii Click on the States tab button.

iv Configure the Administrative State parameter.

v Click on the Channel Group tab button.

vi Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots
  Choose one or more timeslots. You can use the Select All and Deselect All buttons.

vii If you set the Encap Type parameter is set to BCP Null, BCP DOT1 Q, or IPCP in step ii, you can configure the PPP for the timeslot on the Channel Groups tab.

- Click on the More Actions button and choose Edit PPP. The PPP Interface form opens with the General tab displayed.
- Configure the parameters:
  - Period
  - Drop Count
  - Compression
    The Compression parameter is configurable when the DS1 or E1 channel group is on an ASAP MDA in a 7710 SR or 7750 SR.
- Click on the OK button. The PPP Interface form closes and the DS0 Channel Group (Edit) form reappears.

33 Click on the Statistics tab button to view statistical information.

34 Click on the Faults tab button to view information about alarms.

35 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

Procedure 20-45 To configure a DS3/E3 channel as a network interface on a channelized ASAP MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a DS3/E3 channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level.

5 Perform one of the following.

  a If you are configuring an OC-*n* channelized ASAP MDA, right-click on an available port and choose Create Channel from the contextual menu. The Sts SONET Channel (Create) form opens with the General tab displayed; go to step 6.

  b If you are configuring a DS3/E3 channelized ASAP MDA, right-click on an available port and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed; go to step 11.

6 Configure the parameters:

- Local Channel ID
- Description
- Payload Type

7 Click on the States tab button.

8 Configure the Administrative State parameter.

9 Click on the OK button.The Sts SONET Channel (Create) form closes and the STS1 channel appears in the navigation tree under the port of the channelized ASAP daughter card.

10 Right-click on the STS1 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Description
- Configured MAC
- Mode
  You must set the Mode parameter to Network.
- Encap Type
  The only available encapsulation type available in network mode is PPP.
- Speed
  The only available speed is line rate.
- MTU (bytes)
- Load Balance Algorithm

12 Click on the States tab button.

13 Configure the Administrative State parameter.

14 Click on the Apply button. The form displays additional tabs.

15 Click on the Channel tab button.

16 Configure the parameters:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Loop Respond
- Report Alarms

17 Click on the Message Data Link tab button.

18 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 20-7 describes the MDL message options.

Table 20-7 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

19 Click on the OK button. The DS3/E3 or Sts SONET Channel (Create) form closes and a DS3/E3 channel appears in the navigation tree under the port on the channelized ASAP MDA.

Procedure 20-46 To configure an L3 interface on a DS3/E3 channel on a channelized ASAP MDA

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an L3 interface and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a DS3/E3 channel on a channelized ASAP MDA port. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

5 Click on the Policies tab button to configure the policies for the DS3/E3 channel. Perform the following steps.

- **i** Click on the Select button beside the Network Queue Policy Name parameter. The Select Network Queue Policy - DS3/E3 Channel list form opens.
- **ii** Select a network queue policy from the list and click on the OK button. The Select Network Queue Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form reappears.
- **iii** Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - DS3/E3 Channel list form opens.
- **iv** Select an accounting policy from the list and click on the Ok button. The Select Accounting Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form refreshes with the accounting policy information.
- **v** Configure the Collect Accounting Statistics parameter.
- **vi** Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port. The Select Port Scheduler Policy - Physical Port form opens.
- **vii** Select a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

6 Click on the Network Interfaces tab button.

7 Click on the Create button. The Create Network Interface - Routing Instance form opens.

8 Perform steps 4 to 42 of Procedure 30-7 to create a network interface on the DS3/E3 channel.

The port in step 6 of Procedure 30-7 is set to the DS3/E3 channel by default. Go to step 11 of Procedure 30-7.

9 The L3 interface appears on the Network Interfaces tab. Close the Ds3/E3 Channel (Edit) form.

Procedure 20-47 To configure a PVC

PVCs are automatically created by the device when a new L3 interface over ATM is created on the 5620 SAM, and when a new ILMI link is created between ATM interfaces. See Procedure 20-48 for more information about creating ILMI links.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure a PVC and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the channel level and click on a SONET/SDH ATM clear channel. The property form for the channel opens with the General tab displayed.

5 Click on the L3 Interfaces tab button.

6 Choose the appropriate interface from the list and click on the Properties button. The L3 Interface form opens.

7 Click on the ATM tab button.

8 Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

9 Click on the Apply button to save the changes.

10 To view more information about the PVC:

  i Click on the View PVC Connection button. The ATM PVC Connection form opens.

  ii Click on the tab buttons to view information for the ATM PVC connection.

11 Click on the Cancel button to close the ATM PVC Connection form, the L3 Interface form, and the channel form.

Procedure 20-48 To create an ILMI link

Perform this procedure to create an ILMI link between device ATM interfaces. This functionality is supported on the 7750 SR and 7710 SR. Ensure that ATM QoS policies are configured before you create the ILMI link. See chapter 46 for more information about creating ATM QoS policies.

1 Perform one of the following to open the ATM Interface properties form.

a Use the navigation tree

i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

ii Right-click on the device where you want to create an ILMI link and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

iii On the Network Element (Edit) form navigation tree, expand the Shelf icon.

iv Expand to the port level and click on a clear channel port. The Physical Port (Edit) form opens with the General tab displayed.

Note — A clear channel port is a port on a card that is not designated Deep Channelized.

v Click on the Channels tab button.

vi Choose the appropriate channel from the list and click on the Properties button. The Channel (Edit) form opens.

vii Click on the More Actions button and choose Edit ATM. The ATM Interface form opens with the General tab displayed.

b Use the Manage Equipment list form to search for a clear channel port with an ATM interface.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Choose Port from the object drop-down list.

iii Configure the filter criteria to search for ATM encapsulation types.

iv Click on the Search button. The Select form displays the results of the search.

v Select an entry by double-clicking. Alternatively, select an entry and click on the Properties button. The Select form closes and the Channel (Edit) form opens.

vi Click on the More Actions button and choose Edit ATM. The ATM Interface form opens with the General tab displayed.

2 Click on the Create ILMI Link button. The Configure ILMI Link form opens with the General tab displayed.

3 Configure the parameters:

- Administrative Status
- Protocol Version
- IME Type
- Egress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to open the egress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Ingress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to launch the ingress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults
- ILMI Link VCI
- ILMI Link VPI

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Click on the Finish button. The Configure ILMI Link form closes and the ATM Interface form reappears.

5 Close the ATM Interface form. The Channel (Edit) form reappears.

6 Close the Channel (Edit) form.

Procedure 20-49 To modify an ILMI link

1 Perform step 1 of Procedure 20-48 to open the ATM Interface form.

2 Click on the Edit ILMI Link button. The Configure ILMI Link form opens with the ILMI Link Configuration tab displayed.

3 Configure the parameters, as required.

- Administrative Status
- Protocol Version
- IME Type
- Egress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to open the egress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Ingress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to launch the ingress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Click on the Peer Interface Configuration tab to view ILMI properties of the peer interface of the link.

5 Click on the OK button to close the Configure ILMI Link form. The ATM Interface form reappears.

6 To remove an ILMI link, click on the Remove ILMI Link button. Removing the ILMI link also removes the PVC.

Note — An ILMI link can be removed only if its Administrative Status parameter is set to Disabled.

7 Click on the Cancel button to close the ATM Interface form. The Channel (Edit) form reappears.

8 Click on the Cancel button to close the Channel (Edit) form.

21 — NE user and device security

21.1 NE user and device security overview

The 5620 SAM provides security support for accessing managed devices, such as the 7750 SR, as follows:

- create and manage users, profiles and passwords for access to NEs
- configure RADIUS or TACACS+ authentication to control access to the managed devices using 5620 SAM user accounts
- configure device system security through traffic filtering and blocking

RADIUS is an access server AAA protocol. The protocol provides a standardized method of exchanging information between a RADIUS client, which is located on the 7750 SR and managed by the 5620 SAM, and a RADIUS server, which is located externally from the 7750 SR and the 5620 SAM.

RADIUS functionality provides an extra layer of login security. The RADIUS client relays user account information to the RADIUS server. The server authenticates the user and returns user privilege information to the RADIUS client. This determines the level of access that the user has to the device. For example, the user may not be able to FTP information to or from the device.

TACACS+ provides functionality that is similar to RADIUS.

Note 1 — The 5620 SAM server checks for reachability to the TACACS+ server using UDP port 49 to prevent long timeout issues. However, all subsequent communication is over TCP port 49.

Note 2 — You cannot use the 5620 SAM to configure NE security support on the 7250 SAS.

User and group permissions on managed devices

The following general rules apply to managed device users, such as 7750 SR users and groups:

- The authentication settings on the device override any configured and distributed authentication settings on the 5620 SAM. For example, if you configure a user account with SHA authentication, and distribute the account to a device configured to use MD5 authentication, authentication is changed to MD5 for that account.
- The management access and CPM filters applied to the managed device must be manually distributed.
- The system administrator can limit the type of access per managed device, for example, allowing FTP access, but denying console, Telnet, and SNMP access.

- User profiles exist independently of users, and are not in effect until they are linked to a user.
- Create device user accounts as a backup to RADIUS or TACACS+ authentication. If the RADIUS or TACACS+ server fails, or there are user issues on the servers, the 7750 SR user account can be used to access the managed device.

Caution — The 5620 SAM cannot obtain a secret value from an NE during resynchronization. Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret. Do not configure a shared authentication secret directly on a managed NE using another interface, for example, a CLI, or the 5620 SAM cannot synchronize the security policy with the NE.

User and user accounts when combined local and remote authentication is used

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM client GUI user accounts for local authentication on the 5620 SAM server with existing TACACS+ or RADIUS system and users.

Consider the following:

- system administrators can use existing TACACS+ or RADIUS user accounts
- you can create 5620 SAM client user accounts that match the exact TACACS+ or RADIUS user account, for example, if the RADIUS user account is jane, you can create a 5620 SAM user jane
- the 5620 SAM user name can be 1 to 80 characters, flexible enough to match most remote authentication user accounts
- 5620 SAM users already authenticated remotely can log in to 5620 SAM using their RADIUS or TACACS+ passwords
- for 5620 SAM users to be authenticated locally, their account passwords must meet 5620 SAM password requirements, described in this section

For example, for user Jane:

- RADIUS user name is jane and password is accessforjane
- 5620 SAM user name is jane and password is LetJane1In!

When Jane is authenticated by RADIUS, she can log in to the 5620 SAM client by typing in jane and accessforjane. If the RADIUS server was down, and she could not be authenticated remotely, to be authenticated locally Jane must log in to the 5620 SAM client by typing jane and LetJane1In!

RADIUS and TACACS+ policies and permissions

See the appropriate RADIUS and TACACS+ documentation for information about installing, configuring, maintaining lists of users, and managing these authentication servers.

For TACACS+ users, you can specify the following in a user template that is read by the global TACACS+ policy:

- The type of permitted NE access, for example, console, FTP, or both
- A home directory
- A login script that runs when the user logs in

You can enable or disable the user template as required to suit your current global policy requirements.

CPM filters and traffic management

Device CPMs provide dedicated traffic management and queuing hardware for protecting the control plane. You can use CPM filters to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for traffic directed to the CPMs.

Note 1 — The 7705 SAR does not support IPv6 CPM IP filters, queue filters, or MAC CPM IP filters.

Note 2 — There is no partial distribution of CPM IP filter policies to the 7705 SAR. When you distribute a CPM IP Filter policy to a specific 7705 SAR, every entry, property, and value within that policy must be supported by that 7705 SAR, or distribution of that policy is blocked to that 7705 SAR.

The 5620 SAM supports the following CPM traffic management functionality:

- traffic classification using CPM filters
    - Packets going to the CPM are first classified by the IOM into forwarding classes before recognition by the CPM hardware. You can use CPM filters to further classify the packets using L3/L4 information, for example, destination IP, DSCP value, and TCP SYN/ACK.
- queue allocation
    - Queues 1 — 8 are the default queues. They cannot be modified or deleted. Unclassified traffic is directed to the default queues.
    - Queues 9 — 32 are reserved for future use.
    - Queues 33 — 2000 are available for allocation.
    - Queues 2001 — 8000 are used for per-peer queuing.
- queue configuration
    - PIR
    - CIR
    - CBS
    - MBS

DoS protection

The 7750 SR-7, 7750 SR-12, 7450 ESS-7, and 7450 ESS-12 support the use of DoS protection on network and access interfaces. To protect NEs from the high incoming packet rates that characterize DoS attacks, you can use the 5620 SAM to configure DoS protection for the following scenarios:

- the arrival of unprovisioned link-layer protocol packets that are received from CE devices in the core network
- the arrival of excessive subscriber control-plane packets on L2 or L3 access interfaces in aggregation networks
- the arrival of excessive Ethernet CFM frames on L2 and L3 access interfaces, SAPs, and SDP bindings, based on a combination of CFM OpCode and MEG-level values

DoS protection limits the number of packets that are received each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

DoS protection in the core network

DoS protection in the core network limits the number of link-layer protocol packets that each network interface on an NE accepts for protocols that are not enabled on the interface. The interface drops the excessive packets before they are queued or processed by the CPU.

You can configure global DoS protection on an NE using the NE System Security form. DoS protection controls the following for unprovisioned link-layer protocols:

- the packet arrival rate per source on each network interface
- the overall packet arrival rate per source on the NE
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically applies default DoS protection parameters to each network and access interface. These defaults limit only the overall packet arrival rate and apply to all of the interfaces on the NE.

DoS protection policies in aggregation networks

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can configure DoS protection policies to control the following on network interfaces, VPLS L2 access interfaces, and IES and VPRN L3 access interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each network and access interface. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

See Procedure 21-3 for information about creating or modifying a DoS protection policy and assigning the policy to one or more NEs. See the appropriate service chapter for information about applying DoS protection policies to interfaces.

IP security

The 5620 SAM supports the IPsec MDA which provides IP security support including tunneling and encryption functions. See the 7750 SR IP security node documentation for more information about configuring IP security.

21.2 Workflow to manage NE user and device security

Note — 5620 SAM security management support for the OmniSwitch is limited to the configuration of RADIUS and TACACS+ access policies for user authentication.

This workflow describes the procedures for managing NE user and device security.

1. Specify the type of authentication keys used on the device; for example, SHA or MD5. See chapter 14 for more information.

2. Create site management access filter policies for each device from the 5620 SAM. See Procedure 21-1 for more information.

3. Create filter policies for device CPM modules. See Procedure 21-2 for more information.

4. Create site user profiles based on job classifications and the access needed to the managed devices. See Procedure 21-5 for more information.

5. Create individual site user accounts based on the configured profiles. See Procedure 21-6 for more information.

6. As required, manage user profiles and user accounts. See chapter 9 for more information:

    - modify profiles and users
    - delete profiles and users
    - change passwords as specified in the password policy

7. Create RADIUS or TACACS+ policies for user authentication. See Procedure 21-8, Procedure 21-9, and Procedure 21-11 for more information.

8. As required, configure NE system security parameters such as the following:

    - peer queuing for hardware CPM queues
    - enabling or disabling FTP, Telnet, or SSH servers on managed devices
    - RADIUS and TACACS+ user templates
    - global NE DoS protection parameters

    See Procedure 21-10 for more information.

9 Specify password policies for access to managed devices and users. See Procedure 21-7 for more information.

10 Create NE DoS protection policies, as required. See Procedure 21-3 for more information.

11 Create subscriber authentication policies for DHCP sessions, as required. See Procedure 21-12 for more information.

12 Modify the security policies, as required. See Procedure 21-13 for more information.

13 Release and distribute the policies to the managed devices. See Procedure 21-14 for more information.

Note 1 — Before you distribute policies to managed devices, ensure the management access filter Action parameter is not set to deny. Shut down the filter, distribute the policies, and then turn the filter back up.

Note 2 — If the policy is in draft mode, the Distribution option, located under the More Actions button, is disabled and the policy cannot be distributed. You must first release the policy for distribution.

When you change the configuration mode of a management access filter or CPM IP filter to released, the policy is not distributed to existing local definitions. When all other policies are changed to released, the policy is distributed to existing local definitions

14 Delete policies, as required. See Procedure 21-15 for more information.

21.3 NE user and device security procedures

This section provides procedures to create and manage security on the managed devices.

Procedure 21-1 To create or modify a site management access filter policy for a managed device

A site management access filter performs the following functions:

- Restricts the type of management access allowed
- Specifies a strict underlying connection protocol usage and the accepted IP addresses and ports that can gain access to the device

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Management Access Filters from the 5620 SAM main menu. The NE Management Access Filter form opens.

2 Perform one of the following:

a Specify a filter to search for and edit and existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Site Management Access Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Configure the following parameters on the IPv4, IPv6, and MAC panels, as required:

- Default Filter Action
- Administrative State

5 Click on the IPv4 Entries tab button.

6 Perform one of the following.

a Click on the Create button to add a new site entry. The Site MAF Match Entry (Create) form opens.

b Select an entry in the list and click on the Properties button to modify an existing entry. The Site MAF Match Entry (Edit) form opens.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Protocol
- Log
- Router

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

8 Click on the OK button. The Site MAF Match Entry (Create) or Site MAF Match Entry (Edit) form closes.

9 Click on the IPv6 Entries tab button.

10 Perform one of the following.

a Click on the Create button to add a new site entry. The Site IPv6 MAF Match Entry (Create) form opens.

b Select an entry in the list and click on the Properties button to modify an existing entry. The Site IPv6 MAF Match Entry (Edit) form opens.

11 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Next Header
- Log
- Flow Label
- Router

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

12 Click on the OK button. The Site IPv6 MAF Match Entry (Create) or Site IPv6 MAF Match Entry (Edit) form closes.

13 Click on the MAC Entries tab button.

Note — MAC MAF functionality is supported on the 7750 SR, 7450 ESS, and 7710 SR Release 6.1 R4 or later.

14 Click on the Create button. The Site MAC MAF Match Entry (Create) form opens with the General tab displayed.

15 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

16 Click on the Filter Properties tab button.

17 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

18 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 17, configure the following parameters. Otherwise, go to step 19.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to e802dot2SNAP in step 17, configure the following parameters. Otherwise, go to step 19.

- SNAP OUI
- SNAP PID

c If you set the Frame Type parameter to Ethernet II in step 17, configure the Ether Type parameter. Otherwise, go to step 19.

19 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

20 Click on the OK button. A confirmation window appears.

21 Confirm the action.

22 Repeat for each site management access filter you want to create or modify.

> **Note —** If the policy is in draft mode, the Distribution option, located under the More Actions button, is disabled and the policy cannot be distributed. You must first release the policy for distribution. When you switch the configuration mode to released, the policy is not distributed to existing local definitions. See Procedure 21-14 for more information about how to release a policy.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-2 To create or modify a CPM filter policy for a managed device

A device CPM module provides traffic management and queuing hardware for protecting the control plane. The device provides dedicated 10 Gb/s hardware protection for the control planes. You can create CPM filters for the following traffic management functions:

- Drop traffic
- Accept traffic
- Allocate dedicated hardware shaping queues for traffic directed to the control processors

> **Note 1 —** You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure
>
> **Note 2 —** The 7705 SAR does not support IPv6 CPM filters, Queue filters, or MAC CPM filters.

1 Choose Administration→Security→NE CPM Filter from the 5620 SAM main menu. The NE CPM Filter form opens.

2 Perform one of the following steps.

  a Specify a filter to search for and edit and existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

  b Click on the Create button. The CPM Filter (Create) form opens.

3 Click on the General tab button.

4 Configure the parameters as required.

- Displayed Name
- Description
- Default Filter Action
- Administrative State
- IPv6 Administrative Status

Note — The 7705 SAR does not support IPv6 and MAC CPM filters.

5 Click on the IPv4 Entries tab button.

6 Perform one of the following steps.

a Click on the Create button to add a new filter entry.

b Click on an entry in the list and click on the Properties button to modify an existing entry.

The CPM IP Filter Entry (Create) form opens with the General tab displayed.

7 Configure the parameters.

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

8 Click on the Filter Properties tab button.

9 Configure the parameters:

Note — The configurable parameters available depends on the choice of protocol.

- Action
- Protocol
- Queue ID
- DSCP
- Source IP
- Source Mask
- Destination IP
- Destination Mask
- Destination Port
- Routing Instance
- Fragment
- IP Option
- IP Option Mask
- Option Present
- Multiple Option
- ICMP Code
- ICMP Type
- Source Port
- TCP Ack
- TCP Syn

The Queue ID parameter is configurable when the Action parameter is set to queue.

10 Click on the OK button. The new CPM IP filter entry appears in the list.

11 Click on the IPv6 Entries tab button.

12 Perform one of the following steps.

a Click on the Create button to add a new filter entry.

b Select an entry in the list and click on the Properties button to modify an existing entry.

The CPM IPv6 Filter Entry (Create) form opens with the General tab displayed.

13 Configure the parameters.

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

14 Click on the Filter Properties tab button.

15 Configure the parameters:

- Action
- Next Header
- Queue ID
- DSCP
- Source IP
- Source Mask
- Destination IP
- Destination Mask
- Routing Instance
- Flow Label

The Queue ID parameter is configurable when the Action parameter is set to queue.

16 Click on the OK button. The new CPM IPv6 filter entry appears in the list.

17 Click on the MAC Entries tab button.

Note — MAC CPM filters are supported only on the 7750 SR and 7450 ESS, Release 6.1 R4 or later.

18 Perform one of the following steps.

a Click on the Create button to add a new MAC entry. The CPM MAC Filter Entry (Create) form opens with the General tab displayed.

b Select an entry from the list and click on the Properties button to modify an existing CPM MAC entry. The CPM MAC Filter Entry (Edit) form opens with the General tab displayed.

19 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

20 Click on the Filter Properties tab button.

21 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

22 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 21, configure the following parameters. Otherwise, go to step 24.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to Ethernet II in step 21, configure the Ether Type parameter. Otherwise, go to step 24.

23 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

24 Click on the Queues tab button.

25 Perform one of the following steps.

a Click on the Create button to add a new CPM filter queue. The CPM Filter Queue (Create) form opens with the General tab displayed.

b Click on an entry in the list and click on the Properties button to modify an existing CPM filter queue.

26 Configure the parameters.

- ID
- Displayed Name
- Description

27 Click on the CIR/PIR tab button.

28 Configure the parameters.

- CIR (kb/s)
- PIR (kb/s)
- MAX

Ensure that the CIR value is lower than the PIR value.

29 Click on the Burst Size tab button.

30 Configure the parameters.

- Committed Burst Size (KB)
- Maximum Burst Size (KB)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) parameter value is lower than the Maximum Burst Size (KB) parameter value.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The CPM IP Filter (Create) form reappears.

33 Repeat for each CPM filter that you want to create or modify.

34 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-3 To create or modify an NE DoS protection policy

Perform this procedure to control the amount of subscriber-based control-plane traffic that NE interfaces receive.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE DoS Protection from the 5620 SAM main menu. The NE DoS Protection form opens.

2 Perform one of the following.

a Create a policy.

i Click on the Create button. The NE DoS Protection (Create) form opens.

ii Configure the following parameters:

- Auto-Assign ID
- Policy ID

iii Click on the Apply button. The form displays additional buttons and the form name changes to NE DoS Protection (Edit).

b Modify an existing policy.

i Configure the filter criteria. A list of DoS protection policies is displayed.

ii Select a policy in the list and click on the Properties button. The NE DoS Protection (Edit) form opens.

3 Configure the following parameters:

- Description
- Packet Rate Limit (pps)
- Overall Rate Limit (pps)
- Out Profile Rate (pps)
- Receive Notification

4 Perform the following steps to configure CFM frame-rate limiting, if required.

i Click on the CFM Rate Limiting tab button.

ii Click on the Create button. The CfmRateLimiting (Create) form opens.

iii Configure the parameters:

- Policy ID
- Description
- Packet Rate Limit (pps)
- Level Set

iv Click on the Add button in the Op Code Set panel. The Select Property form opens.

Note — You must specify at least one OpCode value.

v Select one or more OpCodes in the list and click on the OK button. The OpCode entries are listed on the CfmRateLimiting (Create) form.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The CfmRateLimiting (Create) form closes.

5 Distribute the policy to NEs, as required, as described in Procedure 21-14.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The NE DoS Protection (Edit) form closes.

Procedure 21-4 To view NE DoS protection violations

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Select a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed.

3 Click on the NE DoS Protection tab button.

4 Perform one of the following to view a specific violation type.

a Click on the Per Source Violations tab button to view a list of the violations that are associated with subscriber hosts.

b Click on the Link Specific Port Violations tab button to view a list of the violations at the port level. The following kinds of violations are listed:

- violations that exceed the Link Rate Limit (pps) parameter value specified for the NE
- violations that exceed the Port Overall Rate Limit (pps) parameter value specified for the NE.

c Click on the Network Interface Violations tab button to view a list of the violations for network interfaces that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

d Click on the SAP Interface Violations tab button to view a list of the violations for SAPs that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

5 Repeat step 4 as required to view another violation type.

6 Close the NE System Security (Edit) form.

Procedure 21-5 To create a user profile for managed device access

A site user profile specifies the commands or command groups that are permitted or denied on the managed device by the 5620 SAM.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Profiles from the 5620 SAM main menu. The NE User Profiles form opens.

2 Click on the Create button. The Site User Profile (Create) form opens.

3 From the General tab, configure the parameters.

- Displayed Name
- Description
- Default Profile Action
- LI Profile

Note — To configure the LI Profile parameter you must have LI privileges. For more information about LI, see chapter 34.

4 Click on the Apply button.

5 Click on the Entries tab button.

6 Click on:

a The Create button to add a new site entry.

b An entry in the table and click on the Properties button to modify an existing entry.

The Site User Profile Match Entry (Create) form opens when you create a new entry.

7 Configure the parameters.

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Match String

Specify the Match String parameter. A match string is a CLI command prefix, which defines the scope of the user profile. For example, when you set the match string to “config” and specify a deny action, this user profile cannot use any CLI commands that begin with the word “config”.

8 Click on the Apply button to save the changes. The site user profile match entry appears in the list form.

9 Verify the action.

10 Click on the OK button to close the form.

11 Repeat for each required site user profile.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-6 To configure a user account for access to a managed device

Perform this procedure to create a user account on a device for managed device access when the authentication servers are unavailable, or to specify the allowed types of device access, for example, Telnet, SNMPv3, FTP, or console.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The NE User (Create) form opens with the General tab displayed.

3 Configure the parameters.

- User Name
- Additional ID
- Description
- Access
- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Note — For SNMP v2 managed NEs, you can create and update an SNMP user configuration policy when SNMP is not enabled for the Access parameter.

4 When a user has console permission, you can configure the parameters in the Console Profiles tab.

i Click on the Console Profiles tab button. The list of profiles numbered one through eight appears.

Each user can have up to eight profiles.

ii Click on the Select button beside Profile 1 and Profile 2 to 8 parameters. Profile 1 is automatically configured to use the system-generated default profile.

The Select Site User Profile form opens. Default profiles and the profiles created in Procedure 21-5 are listed.

iii Choose a profile from the list.

iv Click on the OK button. The profile name appears beside the profile number.

5 When a user has SNMPv3 permissions, you can configure the authentication parameters. Ensure that the SNMPv3 user and user group has been created on the managed device. If MD5 or SHA authentication and DES privacy is used, ensure the keys have been created and associated with the managed device and the SNMPv3 user group, as described in Procedure 14-1.

i Click on the SNMP v3 tab button.

ii Configure the parameters.

- Authentication Protocol
- Privacy Protocol
- New Authentication Password
- Confirm New Auth Password
- New Privacy Password
- Confirm New Privacy Password

iii Click on the OK button to save the changes.

iv Verify the action.

6 Click on the Apply button to save the changes.

7 Close the form.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-7 To create or modify a password policy

Perform this procedure to create a policy that specifies the rules to which a password must conform on one or more devices.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Password Policy from the 5620 SAM main menu. The NE Password Policy form opens.

2 Click on the Create button. The Site Password Policy (Create) form opens.

3 Configure the parameters.

- ID
- Auto-Assign ID
- Name
- Description
- Complexity
- Lockout Time (minutes)
- Password Never Expires
- Maximum Attempts
- Maximum Attempts Time (minutes)
- Days Before Expiration
- Minimum Length
- Health Check
- Health Check Interval
- Authentication Order 1
- Exit On Reject
- Admin Password

If the password can expire, specify the expiration parameter to indicate the number of days that the password can be active before the old password expires and a new password must be set.

Use the Maximum Attempts and Maximum Attempts Time (minutes) parameters to specify the number of attempts allowed within a specified time.

If the maximum number of password attempts in the specified time is exceeded, set how long the account is locked out using the Lockout Time (minutes) parameter.

4 Specify the types and order of password authentication to be used to verify the user account password using the Authentication Order 1 through 3 parameters. Set the order from the most preferred method of authentication to the least preferred method of authentication.

5 Click on the OK button to save the changes.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-8 To create an NE RADIUS access policy

See the appropriate RADIUS documentation for more information about configuring RADIUS servers.

1 Choose Administration→Security→NE RADIUS Authentication from the 5620 SAM main menu. The NE RADIUS Authentication form opens.

2 Click on the Create button. The Site RADIUS Policy (Create) form opens.

3 Configure the parameters.

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Enable Authorization
- RADIUS Authorization Algorithm
- Retry Attempts
- Timeout (seconds)
- Authentication Port
- Source Address
- Accounting Port
- Enable User Template

Note — The Source Address parameter on the Site RADIUS Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the RADIUS server.

4 Click on the Servers tab button to configure a connection to the RADIUS servers. You can configure up to five RADIUS servers.

i Click on the Create button. The Site RADIUS Server (Create) form opens.

ii Configure the parameters.

- ID
- Displayed Name
- Description
- Address
- Secret Name

iii Click on the OK button to save the changes.

5 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 21-14.

Ensure that the authentication order uses RADIUS first. See Procedure 21-7 for more information.

Procedure 21-9 To create an NE TACACS+ access policy

See the appropriate TACACS+ documentation for more information about configuring TACACS+ servers.

See section 9.4 for a sample configuration.

1 Choose Administration→Security→NE TACACS+ Authentication from the 5620 SAM main menu. The NE TACACS+ Authentication form opens.

2 Click on the Create button. The Site TACACS+ Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Accounting Type
- Enable Authorization
- Timeout (seconds)
- Single Connection
- Source Address
- Enable User Template

Note — The Source Address parameter on the Site TACACS+ Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the TACACS+ server.

4 Click on the Servers tab button to configure a connection to the TACACS+ servers. You can configure up to 5 TACACS+ servers.

i Click on the Create button.

The Site TACACS+ Server (Create) form opens.

ii Configure the parameters.

- ID
- Displayed Name
- Description
- Address
- Secret Name

iii Click on the OK button to save the changes.

5 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-10 To configure NE system security

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Select a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed.

3 Click on the Servers Configuration tab button to configure the type of servers that you want to configure on the managed device.

4 Configure the parameters:

- Servers Enabled
- SSH
- Graceful Shutdown
- Minimum TTL Value
- Graceful Shutdown
- Minimum TTL Value

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

5 Click on the CPM-Per-Peer-Queuing tab button to ensure that the managed device allocates a separate CPM hardware queue for the peer, for example, a BGP or T-LDP peer.

6 Configure the CPM Per-Peer-Queuing parameter.

7 Click on the System User Template tab button. The default template is displayed.

8 Select the default template and click on the Properties button. The System User Template (Edit) form opens.

9 Configure the parameters.

- Access
- Home Directory
- Restricted to Home Directory
- Console Login Exec File

10 Click on the OK button. The System User Template (Edit) form closes.

11 Click on the NE DoS Protection tab button to configure global DoS functionality for the NE.

12 Configure the parameters:

- Link Rate Limit (pps)
- Port Overall Rate Limit (pps)
- Protection Administrative State
- Allow Sham Links

13 Click on the following tab buttons to view violations information, as required. See Procedure 21-4 for more information.

- Per Source Violations
- Link Specific Port Violations
- Network Interface Violations
- SAP Violations

14 Click on the Faults tab button to view alarm information, as required.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The NE System Security (Edit) form closes.

You must distribute policies to specific devices, as described in Procedure 21-14.

Procedure 21-11 To create an OmniSwitch RADIUS or TACACS+ security policy

See the appropriate RADIUS or TACACS+ documentation for information about configuring RADIUS and TACACS+ servers.

1 Choose Administration→Security→NE AOS Security Authentication from the 5620 SAM main menu. The NE AOS Security Authentication form opens.

2 Click on the Create button. The Site AOS Security Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Protocol Name

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

a If you set the Protocol Name parameter to RADIUS in step 3, go to step 5.

b If you set the Protocol Name parameter to TACACS+ in step 3, go to step 8.

5 Configure the parameters.

- IP Address
- IP Address 2
- Time Out
- Retries
- Secret
- Authentication Port
- Account Port

6 Click on the Apply button to save the changes.

7 To configure multiple RADIUS servers, repeat steps 3 to 4 to add more RADIUS servers; otherwise go to step 11.

8 Configure the parameters:

- IP Address
- IP Address 2
- Time Out
- Secret
- Port

9 Click on the Apply button to save the changes.

10 To configure multiple TACACS+ servers, repeat steps 3 to 4 to add more TACACS+ servers; otherwise go to step 11.

11 Close the Site AOS Security Policy (Create) form.

You must distribute the security policies to specific devices, as described in Procedure 21-14.

Ensure that the authentication order uses RADIUS first. See Procedure 21-7 for more information.

Procedure 21-12 To create a subscriber authentication policy

The 5620 SAM provides security support for creating DHCP sessions on the 7450 ESS, 7750 SR, and 7710 SR. The 5620 SAM allows you to create a policy that uses RADIUS authentication to grant network access to a dynamic host. You can apply the policy to a VPLS or IES SAP, or to a VPRN or IES group interface. Authentication is not performed for statically provisioned hosts.

Perform this procedure to create a DHCP-based subscriber authentication policy that defines the parameters for dynamically created subscriber host sessions and authenticates the sessions. The 5620 SAM supports up to 32 subscriber authentication policies.

See chapter 71 for information about configuring a VPLS and chapter 73 for information about configuring an IES.

1 From the 5620 SAM main menu, choose Administration→Security→Subscriber Authentication Policy Manager. The Subscriber Authentication Policy Manager form opens.

2 Click on the Create button. The Subscriber Authentication Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Retry Attempts
- Timeout (seconds)
- Re-Authenticate When DHCP Lease Expires
- Accept CoA
- Access Algorithm
- RADIUS Attributes
- Source Address
- PPPoE Access Method
- Authentication Hold Down Time
- User Name Format
- Append To User Name
- Password
- Calling Station ID Type
- Port Type
- Port Type Value
- Port Prefix Type
- Port Prefix String
- Port Suffix Type
- Fallback Action

Note — The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type parameter is set to Config.

The Port Prefix Type, Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

4 Configure the Router Instance parameter. If you set the parameter value to VPRN, go to step 5. Otherwise, go to step 7.

5 Configure a VPRN service as a virtual router instance for the subscriber authentication policy. Perform the following steps.

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Subscriber Authentication Policy list form opens.

ii Select a VPRN site from the list and click on the OK button. The Select VPRN ID - Subscriber Authentication Policy list form closes and the Subscriber Authentication Policy (Create) form refreshes with the VPRN service information.

Note — You must select a VPRN site before you add RADIUS servers in step 7.

6 If you want to configure PAP/CHAP user name re-writing, configure the following parameters:

- User Name Operation
- Domain Name

7 Click on the RADIUS Servers tab button, if required. Otherwise, go to step 12.

8 Click on the Create button. The RadiusEntry (Create) form opens with the General tab displayed.

9 Configure the parameters.

- ID
- Auto-Assign ID
- Description
- Address
- Port
- CoA Only
- Secret Name

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The RadiusEntry (Create) form closes and the Subscriber Authentication Policy (Create) form refreshes with the RADIUS server information displayed in a list in the RADIUS Servers tab.

12 Click on the Apply button. The Subscriber Authentication Policy (Create) form refreshes with additional buttons and tabs.

13 Click on the More Actions button and choose Distribute to manually distribute the policy to the selected devices.

See Procedure 21-14 for information about distributing security policies. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — If the policy is in draft mode, the Distribution option is disabled and the policy cannot be distributed. You must first release the policy for distribution. When you switch the configuration mode to released, the policy is distributed to existing local definitions. See Procedure 21-14 for more information about how to release a policy.

14 Close the Subscriber Authentication Policy (Create) form. The Subscriber Authentication Policy Manager form refreshes with the policy information displayed in a list.

Procedure 21-13 To modify a security policy

1 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

2 Set the filter criteria, if applicable. You can filter or local or global policies by using the Policy Scope parameter. When you set the parameter to Local, you can search on a specific managed device by clicking on the Select button beside the Local Node IP Address parameter.

3 Click on the Search button. A policy list opens.

4 Specify whether to modify the global or the local instance of the policy.

- **a** Local policies have a check mark for the Local column.
- **b** Global policies do not have a check mark for the Local column.

5 Choose a policy from the list.

6 Click on the Properties button.

7 Configure the policy parameters, as required.

From either a local or global policy, you can click on the Local Definitions or Global Definitions tab button to view the local instances of policies or the global policy used to define the local instance.

8 Save the changes and close the file. You must distribute global policies to the managed devices. You do not distribute modified local policies.

Procedure 21-14 To distribute a security policy

1 Create policies, as described in Procedures 21-1 to 21-12.

2 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

3 Set the filter criteria, if applicable.

4 Click on the Search button. A policy list opens.

5 When:

a A management access filter is configured to deny access to managed devices, ensure the following:

i List the applicable management access filters. A list of management access filters opens.

ii Shut down the management access filter.

iii Distribute the policies. Complete steps 6 to 14.

b If no management access filter is configured, go to step 6.

6 Choose a policy from the list.

7 Click on the Properties button if you are distributing a CPM IP, NE DoS protection, or management access filter. The *Policy_Type*, Global (Edit) form opens.

8 When the policy is in draft configuration mode, the Distribute option, located under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing the following steps. Otherwise, go to step 9.

i Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

ii Click on the Yes button. The configuration mode of the policy is changed to Released.

Warning — When you change the configuration mode of a management access filter or CPM IP filter to released, the policy is not distributed to existing local definitions. When all other policies are changed to released, the policy is distributed to existing local definitions.

iii View the local policy, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local policy in the list.

iv Close the local policy form.

9 Click on the More Actions button and choose Distribute. The Distribute form opens.

10 Choose a row or rows from the Available Nodes list.

11 Click on the right arrow button. The chosen device or devices move to the Selected Nodes panel on the right side of the form.

12 Click on the More Actions button and choose Distribute. CPM IP and management access filters require that you confirm the policy distribution. The policy is distributed to the device or devices.

13 Close the Distribute form. The *Policy_Type*, Global (Edit) form reappears.

14 Configure the distribution mode of the local definitions by performing the following steps.

i Click on the More Actions button and choose Distribution Mode. The Distribution Mode - *Policy* form opens.

ii Configure the Distribution Mode parameter. The existing local definitions that are configured with the selected distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow button. The chosen device or devices move to the Selected Nodes panel on the right side of the form.

v Depending on the distribution mode of the chosen device or devices, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Distribution Mode - *Policy* form. The *Policy_Type*, Global (Edit) form reappears.

15 Turn up the management access filter if you performed step 5 a ii. Otherwise, go to step 16.

16 Close the *Policy_Type*, Global (Edit) form.

17 Close the policy manager form.

Procedure 21-15 To delete a security policy

Note 1 — When you delete site management access filter policies in which the Action parameter is set to deny, ensure that you edit the policy to set the parameter to permit before it is deleted, otherwise, the 5620 SAM may be isolated.

Note 2 — You cannot remove a site management access filter if the filter administrative state is up and the default action of the filter is set to deny or deny host unreachable.

Note 3 — If you attempt to delete an OmniSwitch RADIUS or TACACS+ security policy that has been applied to an authentication service, the 5620 SAM generates a deployment error. You must use the OmniSwitch CLI to delete the policy from the authentication service before you can delete the policy from the 5620 SAM.

1 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

2 Set the filter criteria, if applicable.

3 Click on the Search button. A policy list opens.

4 Choose a policy from the list.

5 Click on the Delete button.

6 Click on the Yes button. The policy is deleted.

22 — Inventory management

22.1 Inventory management overview

The 5620 SAM client GUI provides multiple ways of generating inventory data about managed devices and the managed network. You can also use the 5620 SAM-O interface to generate inventory data. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

Use the list, properties, and equipment management forms to generate inventories for:

- required data for SLA audits
- equipment, such as cards, needed for sparing
- installed and in-operation equipment
- vintages, CLEI codes, and identifications

You can generate inventory data based on:

- the entire managed network, which includes all 5620 SAM-managed devices
- a managed device

Note — Not all columns in the inventory lists are applicable to all equipment types. For example, not all card types have an associated CLEI code. In situations such as this, the inventory list displays "N/A" in the column.

Figure 22-1 shows how to use the Manage Equipment form to filter and inventory data for all managed devices.

Figure 22-1 Generating inventory data for all managed devices

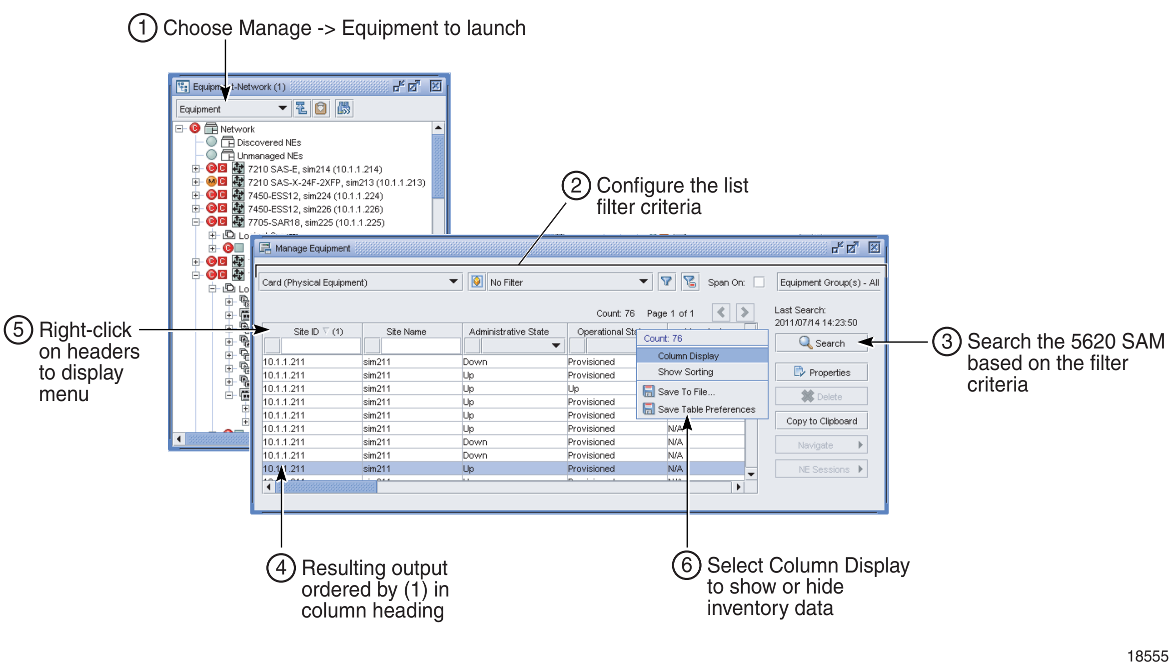
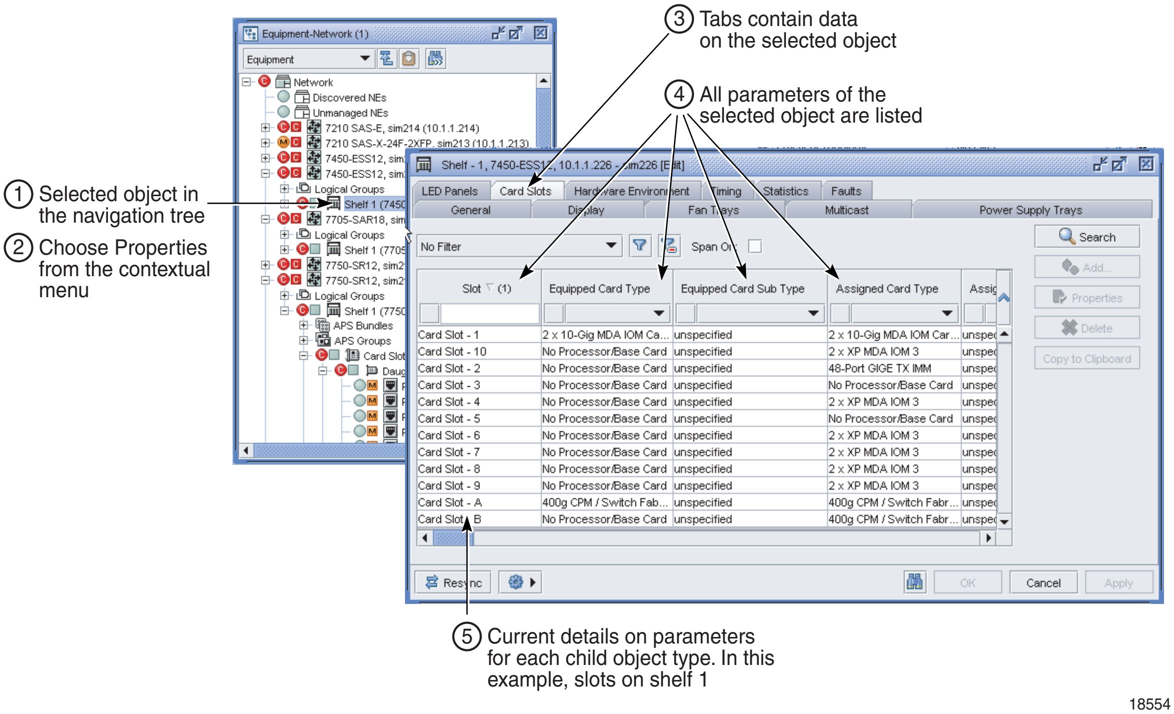


Figure 22-2 shows how to use the properties form for a network object, in this case a shelf on a managed device, to inventory data for the managed device.

Figure 22-2 Generating inventory data for a managed device



Save the data in CSV or HTML format. You can use the saved file for further processing on another platform; for example, as input to a back-office parts management system. Figure 22-3 shows the output of an inventory list saved in CSV format.

Figure 22-3 CSV inventory output

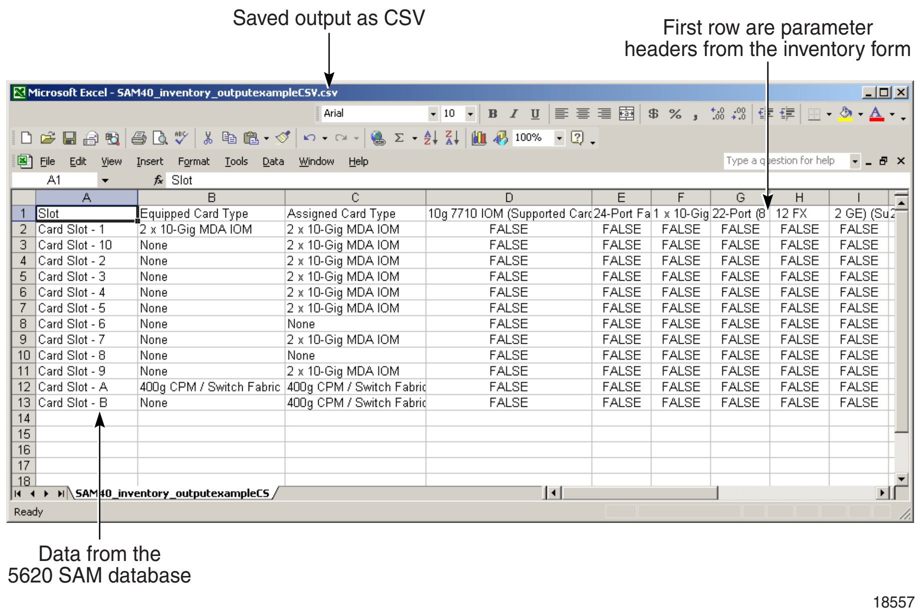
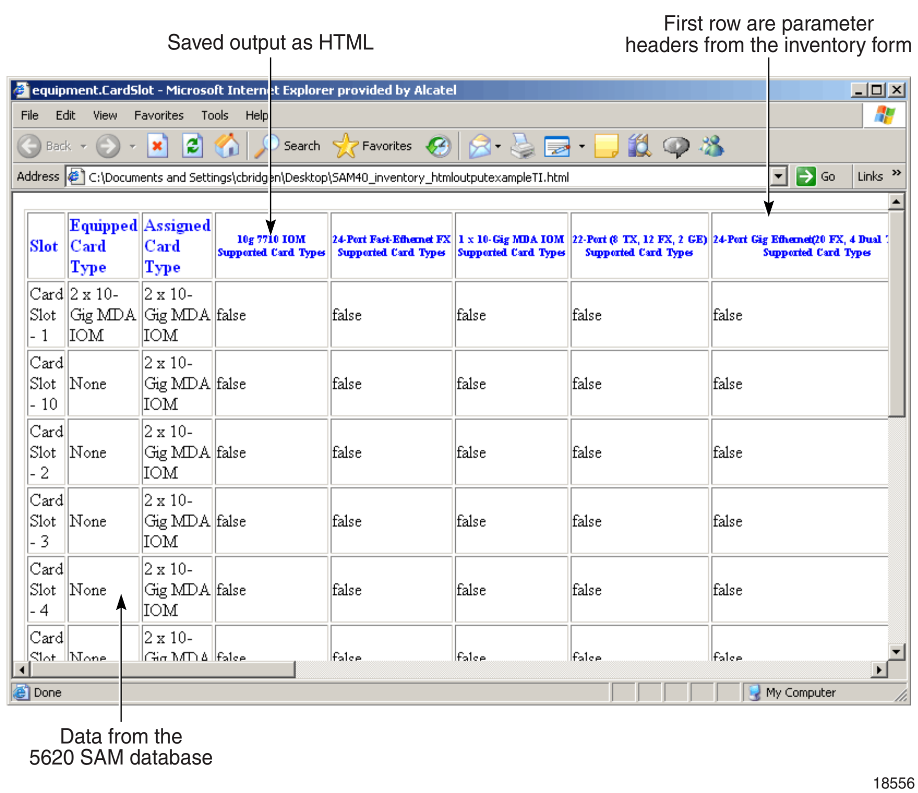


Figure 22-4 shows the output of an inventory list saved in HTML format.

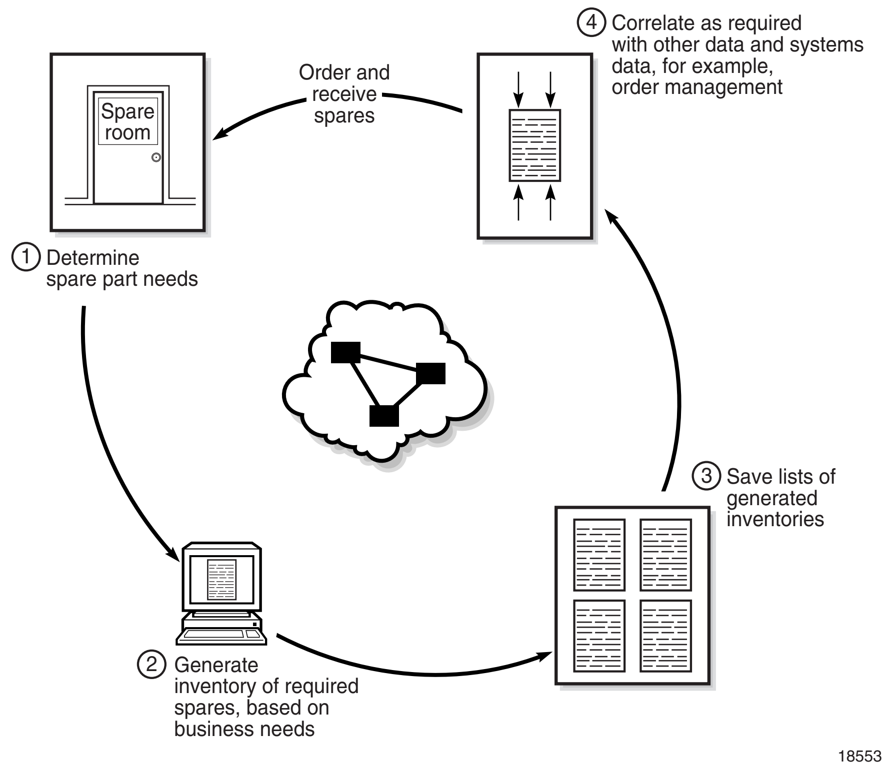
Figure 22-4 HTML inventory output



22.2 Sample inventory management workflow

Figure 22-5 shows an example of an inventory management workflow using the client GUI to generate a list of required spare parts, based on business needs.

Figure 22-5 Example of an inventory management workflow



This example is configured using the following high-level tasks.

1. Determine spare part needs based on business needs and future growth plans.
2. Using the 5620 SAM, generate inventory lists of required spares, keeping in mind the following points.
   - Filter the list form to list only those objects that you want; for example, cards of a certain type required for sparing.
   - Generate multiple lists, based on business needs.
3. Using the 5620 SAM, save lists of required spares in a format compatible with your back-office systems; for example, CSV or HTML. Move the lists to another system, as required by the back-office applications; for example, an order management or data management system.
4. Correlate inventory lists with data from other back-office systems, as required by business needs.

22.3 Workflow for inventory management

1. Determine inventory management needs.
2. Provide inventory management list requirements to NOC operators.
3. As required, generate inventory lists for a managed device or for the entire network. See Procedure 22-1 for more information.
4. As required, generate inventory lists for a managed device from the 5620 SAM client GUI:
    - a Generate inventory lists for CLEI codes. See Procedure 22-5 for more information.
    - b Generate inventory lists for card software versions. See Procedure 22-6 for more information.
    - c Generate inventory lists for port types. See Procedure 22-7 for more information.
    - d Generate inventory lists for shelf data. See Procedure 22-8 for more information.
5. As required, generate inventory lists for the entire network from the 5620 SAM client GUI:
    - a Generate inventory lists for all managed cards. See Procedure 22-9 for more information.
    - b Generate inventory lists for all managed fan trays. See Procedure 22-10 for more information.
    - c Generate inventory lists for all managed flash memory. See Procedure 22-11 for more information.
    - d Generate inventory lists for all managed physical links. See Procedure 22-12 for more information.
    - e Generate inventory lists for all managed ports. See Procedure 22-13 for more information.
    - f Generate inventory lists for all managed power supply trays. See Procedure 22-14 for more information.
    - g Generate inventory lists for all managed processors. See Procedure 22-15 for more information.
    - h Generate inventory lists for all managed shelves. See Procedure 22-16 for more information.
    - i Generate inventory lists for all management ports. See Procedure 22-17 for more information.
    - j Generate inventory data for network device SLA audits. See Procedure 22-18 for more information.
6. As required, save search filters. See Procedure 22-4 for more information.

7 As required, save inventory lists in the required formats:

a Save inventory lists in HTML format. See Procedure 22-2 for more information.

b Save inventory lists in CSV format. See Procedure 22-3 for more information.

8 Move inventory lists to other platforms for post-processing.

22.4 Inventory management procedures

Use the following procedures to perform inventory management tasks.

Procedure 22-1 To list and sort inventory data

Perform this procedure to list and sort inventory data for a device or for the entire network.

1 Inventory can be listed and sorted for a device or for the entire network.

a To list and sort inventory for a device, perform steps 2 to 6.

b To list and sort inventory for the entire network, perform steps 7 to 11.

2 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

3 Choose a Network Element (Network) from the object drop-down list and click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab button and choose a network object from the object drop-down list. The list form displays the results of the inventory search for the selected device.

6 Go to step 11.

7 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

8 Choose a network object from the object drop-down list.

9 Configure the filter criteria.

10 Click on the Search button. The list form displays the results of the inventory search.

11 Sort the results.

a To count the number of items in the list, generate an inventory of data and right-click on the list heading. The Count shows the number of objects in the list.

b To sort in ascending or descending order, click on the column heading. The arrow direction changes to indicate the order in which the data is sorted.

c To move a column, click on the column, drag the column to the right or left, and drop the column in its new location.

d To remove a column,

i Right-click on the column heading and choose Column Display from the contextual menu. The Column Display window appears.

ii In the Displayed on Table list box, choose the columns that you need to remove from the table and click the left arrow. The specified columns are moved to the Available for Table list box.

iii Click on the OK button to apply the changes and close the Column Display window. The specified columns are removed from the table.

e To sort multiple columns, right-click on a column heading and choose Show Sorting from the contextual menu. The Show Sorting form opens. Choose the property or properties from the Available for Sorting panel and click on the right arrow button. The property or properties appear in the Used for Sorting panel. Click on the Sort Ascending or Sort Descending button, as required.

12 Save the inventory output by performing Procedure 22-2 or 22-3.

13 Close the form.

Procedure 22-2 To save inventory output in HTML format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 22-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

i To choose a directory in which to save the listed information, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose HTML (*.htm, *.html) from the Files of Type drop-down menu.

iv Click on the Save button. The results of the inventory search are saved to the specified HTML file.

4 Close the form.

Procedure 22-3 To save inventory output in CSV format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 22-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

i To choose a directory in which to save the listed information, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose CSV (*.csv) from the Files of Type drop-down menu.

iv Click on the Save button. The results of the inventory search are saved to the specified CSV file.

4 Close the form.

Procedure 22-4 To save a filter

See Procedure 3-37 for more information.

Procedure 22-5 To inventory CLEI codes for managed device objects

1 You can list CLEI codes for card slots, cards, daughter card slots and daughter cards.

a To view CLEI codes for a device, perform steps 2 to 7.

b To view CLEI codes for the entire network, perform steps 8 to 13.

2 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

3 Choose a Network Element (Network) from the object drop-down list and click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab button and choose a network object from the object drop-down list. For example:

- To display the cards and daughter cards that are configured in the slots expand Slot (Physical Equipment and select one of the following:
  - Card Slot (Physical Equipment)
  - Daughter Card Slot (Physical Equipment)
- To display the IOMs that are installed on, pre-provisioned, or provisioned for the node expand Card (Physical Equipment) select IO Card (Physical Equipment)

In each instance, the list form displays the results of the inventory search for the selected device.

6 To obtain a list of CLEI codes for the network object selected in step 5, perform step 11d of Procedure 22-1 to remove all columns from the list except for the object ID or object type and the CLEI code columns.

7 Go to step 12.

8 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

9 Choose a network object from the object drop-down list.

10 Click on the Search button. The list form displays the results of the inventory search.

11 To obtain a list of CLEI codes for the network object selected in step 5, perform step 11d of Procedure 22-1 to remove all columns from the list except for the site ID, object ID, and CLEI code columns

12 Save the CLEI code inventory output.

a To save the results in HTML format, perform steps 2 and 3 of Procedure 22-2.

b To save the results in CSV format, perform steps 2 and 3 of Procedure 22-3.

13 Close the form.

Procedure 22-6 To inventory card software versions for a managed device

You can inventory card software versions for a managed device.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab button and choose Card (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 To obtain a list of card software versions for the selected device, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Slot ID
- Software Version

7 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

8 Close the form.

Procedure 22-7 To inventory port types for a managed device

Perform this procedure to generate an inventory of port types, such as physical ports, SONET channels, link aggregation groups, terminations, TDM channels, protocols, multilink bundles, and APS groups.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab button and choose Port (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 To display more detailed port inventory information expand to the following sub-objects on the object drop-down list:

- SONET Channels
- Link Aggregation Groups
- TDM Channels
- Multilink Bundles
- APS Groups

7 To sort the inventory output, perform step 11 of Procedure 22-1.

8 Save the inventory output.

- **a** To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.
- **b** To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

9 Close the form.

Procedure 22-8 To inventory shelf data for a managed device

Perform this procedure to generate an inventory of shelf manufacturer information, part numbers, serial numbers, CLEI codes, and CLLI codes for the shelves of a managed device.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Click on the Search button. The list form displays the results of the inventory search.

4 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

5 Click on the Inventory tab button and choose Shelf (Physical Equipment) from the object drop-down list. The list form displays the results of the inventory search.

6 Choose a shelf from the list and click on the Properties button. The Shelf (Edit) form opens with the General tab button displayed.

7 Click on the Display tab button. A picture of the selected shelf is displayed.

8 Use screen capture software to record the screen image, or otherwise copy the shelf information to a file for further processing.

Note — You can generate an inventory of shelf data for the managed network, but not for an individual managed devices. See Procedure 22-16 for more information.

9 Close the form.

Procedure 22-9 To inventory all managed cards

You can inventory all managed cards in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Card (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of card-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Manufacture Date
- Part Number
- Serial Number
- CLEI Code

6 Save the inventory output.

  a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

  b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-10 To inventory all managed fan trays

You can inventory all managed fan trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Fan Tray (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of fan tray-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- Device State

6 Save the inventory output.

   a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

   b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-11 To inventory all managed flash memory

You can inventory all managed flash memory in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Flash Memory (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of flash memory-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Serial Number
- Firmware Revision
- Model Number
- Capacity (sectors)
- Amount Used (sectors)

6 Save the inventory output.

   a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

   b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-12 To inventory all managed physical links

You can inventory all managed physical links in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link (Network) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of physical link-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Endpoint A Type
- Endpoint A - Port
- Endpoint B Type
- Endpoint B - Port

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-13 To inventory all managed ports

You can inventory all managed ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Port (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of port-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Name
- CLI Name
- MTU (bytes)
- State

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-14 To inventory all managed power supply trays

You can inventory all managed power supply trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Power Supply Tray (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of power supply tray-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Administrative State
- Operational State
- AC Voltage Status
- DC Voltage Status
- Assigned Type

6 Save the inventory output.

  a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

  b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-15 To inventory all managed processors

You can inventory all managed processors in a network of managed devices.

Note — The eNodeB, 9471 MME, and 5780 DSC have distinct types of control cards. See the *5620 SAM LTE RAN User Guide* for information about performing inventory tasks for the eNodeB. See the *5620 SAM LTE ePC User Guide* for information about performing inventory tasks for the 9471 MME and 5780 DSC.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Processor (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of processor-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- CLEI Code
- Manufacturer
- Manufacture Date
- Part Number
- Serial Number

6 Save the inventory output.

  a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

  b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-16 To inventory all managed shelves

You can inventory all managed shelves in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Shelf (Physical Equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of shelf-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- Operational State
- Administrative State
- CLEI Code
- Manufacturer
- Manufacture Date
- CLLI Code
- Part Number
- Serial Number (Manufacturer Details)

6 Save the inventory output.

 a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

 b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the form.

Procedure 22-17 To inventory all management ports

You can inventory all management ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (Network) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 To obtain a list of management port-specific codes, perform step 11d of Procedure 22-1 to remove all columns from the list except for the following:

- System ID
- Management IP Address
- Location
- Chassis Type
- Sys Object ID
- Software Version
- Descriptor Version (software release)
- Resource Group ID

6 Save the inventory output.

 a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

 b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

7 Close the Manage Equipment form.

Procedure 22-18 To collect inventory data for network device SLA audits

You can create lists of inventory data to provide the specific summary information required for SLA audits. Ensure the following before you start:

- Inventory collection requirements differ based on SLA agreements. Ensure that the correct data is being collected for your SLA agreement.
- Perform inventory collection during a maintenance window, or during low network activity windows to ensure no impact to systems.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Collect the required SLA audit data.

a For card SLA audits, choose Card (equipment) from the object drop-down list.

b For shelf SLA audits, choose Shelf (equipment) from the object drop-down list.

c For power supply tray SLA audits, choose Power Supply Tray (equipment) from the object drop-down list.

3 Click on the Search button. The SLA audit data appears in the list.

4 Typically, only a subset of data is required for SLA audits. To display only the required information, perform the following:

i Left-click on the list column heading. The list contextual menu appears.

ii Ensure the information that you want displayed has a check mark. These typically include:

- Identification information, such as Site ID, Site Name, Slot ID, and Slot Name
- SLA audit and ordering information, such as Manufacture Date, Part Number, Serial Number, CLEI Code, and Card Type

iii Close the list contextual menu. Only the chosen information is displayed in the list.

iv Choose Save Table Preferences from the list contextual menu to save the refined list for future use. When a similar search from the same client GUI is performed, the refined list is shown by default.

v Confirm the action.

5 Save the inventory output.

   a To save the output in an HTML file, perform steps 2 and 3 of Procedure 22-2.

   b To save the output in a CSV file, perform steps 2 and 3 of Procedure 22-3.

6 Close the form.

23 — NE maintenance

23.1 NE maintenance overview

The 5620 SAM includes NE maintenance functionality for supported devices that allows a system administrator to:

- define the 5620 SAM deployment and local device configuration-save conditions
- perform an on-demand or scheduled NE configuration backup
- restore a previous device configuration
- perform an on-demand or scheduled NE software upgrade; scheduled software upgrades are supported for the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7210 SAS-E, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 9500 MPR.
- view the status of a deployment, backup, device configuration restore, device software upgrade, or accounting statistics retrieval operation in progress
- troubleshoot a failed deployment, backup or upgrade

A 5620 SAM operator with an administrator or network element software management scope of command role and can perform device configuration save, backup, or restore operations, and can create policies for scheduling backups and configuration saves.

A 5620 SAM operator can upgrade software or schedule a software upgrade on sites and routers that are within their span of control.

A 5620 SAM operator with lawful intercept management scope of command role can perform back up and restore operations for LI configuration on an NE. Back up data is saved only when the LI local save allowed parameter is set to True. See Procedure 13-10 for more information about configuring LI local save allowed.

Managing NE deployments

When you apply a device configuration change using the 5620 SAM—for example, by clicking on OK or Apply after changing a service parameter—the 5620 SAM deploys the configuration change to the device according to the 5620 SAM deployment policy. The 5620 SAM deployment policy also specifies when the device saves its configuration locally. The information in a deployment policy includes the following:

- the number and frequency of deployment retries that the 5620 SAM performs
- the conditions under which the 5620 SAM initiates a device configuration save, such as the frequency and level of saved configuration detail

In a lab or testing environment, it is sometimes necessary to disable 5620 SAM deployment. See the *5620 SAM XML OSS Interface Developer Guide* for information about disabling 5620 SAM deployment.

Managing NE backups and restores

A 5620 SAM backup policy specifies the conditions under which the 5620 SAM performs a device backup to ensure that the device configuration is not lost in the event of a failure. A default policy that is assigned to all managed devices is in place after 5620 SAM installation. You can create and configure multiple backup policies, and you can assign them to multiple NEs. You cannot delete a backup policy that is assigned to an NE. The information in a backup policy includes the following:

- the frequency of backups
- the files that a backup collects
- the type of file compression that the 5620 SAM uses
- the age and number of backup files that the 5620 SAM retains

The 5620 SAM stores the backed-up device configuration files in the 5620 SAM database for ease of tracking and retrieval. You can perform an on-demand export of backup files from the database to a file system, and can import NE backups from a file system to the 5620 SAM database.

You can configure the 5620 SAM to save device configuration backup files to the main-server file system, in addition to the 5620 SAM database, by editing a main-server configuration file. The saved files are synchronized between the primary and standby main servers in a redundant 5620 SAM deployment.

You can configure the 5620 SAM to do the following:

- automatically save device backups to a file system in addition to the database
- automatically delete device backup files after the associated NE is unmanaged

See chapter 6 for more information.

When a device configuration requires replacement, for example, because it becomes corrupted, you can restore a previously backed-up configuration. Unless otherwise specified, the 5620 SAM restores the most recent device configuration backup. See Procedures 23-4 and 23-5 for more information.

Managing NE software upgrades

When a new device software version is available, you can use the 5620 SAM to perform an on-demand NE software upgrade or schedule one using a software upgrade policy. You can create and configure multiple software upgrade policies and assign them to multiple NEs. You cannot delete a software upgrade policy that is assigned to an NE. The information in a software upgrade policy includes the following:

- the NE file location of the currently active device software
- the NE file location in which to store a backup copy of the current device software
- whether to activate the software after transferring it to the NE
- whether to reinitialize the NE after the upgrade
- whether the upgrade is an in-service software upgrade, or ISSU

During a software upgrade, the 5620 SAM performs checks to ensure that the new software is compatible with the device type and that the required files are present. The 5620 SAM does not initiate a device software upgrade unless the necessary conditions are in place. You can use the 5620 SAM to roll back a software upgrade to the previous version in the event of an upgrade failure.

Note — The 5620 SAM does not support a software upgrade or downgrade on a Telco, 7250 SAS, 7250 SAS-ES or 7250 SAS-ESA NE. You can use a software upgrade policy to upload a software image to the NE, but the upgrade or downgrade must be performed using a CLI. Contact your Alcatel-Lucent technical support representative for information about downgrades.

See Procedures 23-11 and 23-14 for more information.

ISSUs

An ISSU on a managed device that has dual CPMs allows the device to provide uninterrupted service during the upgrade process. A device software upgrade requires a CPM restart, which causes temporary device down time. When a device has dual CPMs, however, one CPM can remain active while the other restarts with the upgraded software. These alternate CPM restarts mean that the device remains in service during the upgrade. If an upgrade on a CPM fails, the CPM reports a failed state and raises an alarm. In-service software upgrades for devices are restricted to maintenance software releases.

You can specify that the 5620 SAM activates the new software image immediately after transferring it to an NE, or you can specify only the file transfer and manually activate the software image later. Manual software activation provides more control over an upgrade, which may be required, for example, when multiple NEs are involved.

NE file-system browsing

A 5620 SAM operator can browse the file system of a managed NE to list the contents of the compact flash devices. You can browse the file system of a 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7705 SAR, 7710 SR, or 7750 SR using simple FTP or a CLI session using SSH. The 5620 SAM GUI is used to browse the different types of files.

Browsing an NE file system using the 5620 SAM is a convenient way to confirm that operations such as the following occur as planned by verifying the sizes and time stamps of local NE files:

- NE configuration saves
- NE software image transfers and upgrades
- NE configuration restores
- NE accounting-statistics collection

FTP file browsing on an NE requires FTP user-account access on the NE. SSH file browsing requires console user-account access and the configuration of SSH security on the NE. See chapter 14 for information about enabling FTP or console access for an NE user account. See chapter 14 for information about configuring SSH on an NE.

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

See Procedure 23-26 for information about browsing an NE file system using an FTP file browser. See Procedure 23-27 for information about browsing an NE file system using an SSH file browser.

Secure file transfers for site backups and upgrades

The 5620 SAM supports secure and non-secure file transfers for backups, restores, software upgrades, and statistics collection. The device mediation policy determines whether FTP or SCP is used to perform file transfers to and from the managed devices. See chapter 14 for information about configuring SSH2.

The following devices support the use of SSH2 for secure file transfers:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6850E
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E

Sample deployment policy configuration

The following example describes the configuration and operation of a 5620 SAM deployment policy. The example uses the default parameter values, which are appropriate for most applications. The Deployment Policy properties form contains the parameters listed in the example. See Procedure 23-1 for deployment configuration information.

Example details

The sample deployment policy specifies that after a configuration deployment failure, the 5620 SAM retries the deployment until it is successful. The policy also specifies that the 5620 SAM initiates a save of the device configuration to local storage after every configuration change. In order to conserve storage space, the device is configured to save the configuration information for only the device parameters that are not at their default values.

The deployment policy parameters and their values for the example are:

- Auto Save Scheme—Every Deployment
- Auto Save Threshold—0
- Scheduled Save Scheme—None
- Scheduled Save Interval—1 hour
- Save Details—disabled
- Retry Scheme—Retry Forever
- Retry Interval—5 minutes
- Retry Threshold—0

Sample backup/restore policy configuration

The following example describes a sample 5620 SAM backup/restore policy configuration and its operation using parameter values that are appropriate for most applications. The Backup Policy form contains the parameters listed in the example. See Procedure 23-3 for the configuration information.

Example details

The sample backup policy specifies that the 5620 SAM obtains the backup files by FTP from the device once every hour regardless of configuration activity, and after every 25 configuration changes. The policy also specifies that the 5620 SAM backs up the device configuration file and boot options file (BOF) only when a newer file is present, and uses gzip file compression. The 5620 SAM is to retain at most 30 backup versions, and purge versions that are more than 30 days old.

The backup policy parameters and their values are:

- Enable Backup—enabled
- Auto Reboot After Successful Restore—enabled
- Scheduled Backup Scheme—Every Scheduled Interval
- Scheduled Backup Interval—1 hour
- Scheduled Backup Sync Time — 00:00
- Scheduled Backup Threshold (operations)—5
- Auto Backup Scheme—Every Nth 5620 SAM Server Initiated Save
- Auto Backup Threshold (operations)—50
- CLI Config File Mode—New Version Only
- CLI Config Save Details—disabled
- CLI Debug Save Config File Mode—disabled
- Boot Option File Mode—New Version Only
- File Compression—GZIP
- Auto-Purge Scheme—By Age But Retain A Minimum Number Of Backups
- Number of Backups—30
- Maximum Backup Age (days)—30

Figure 23-1 5620 SAM backup process

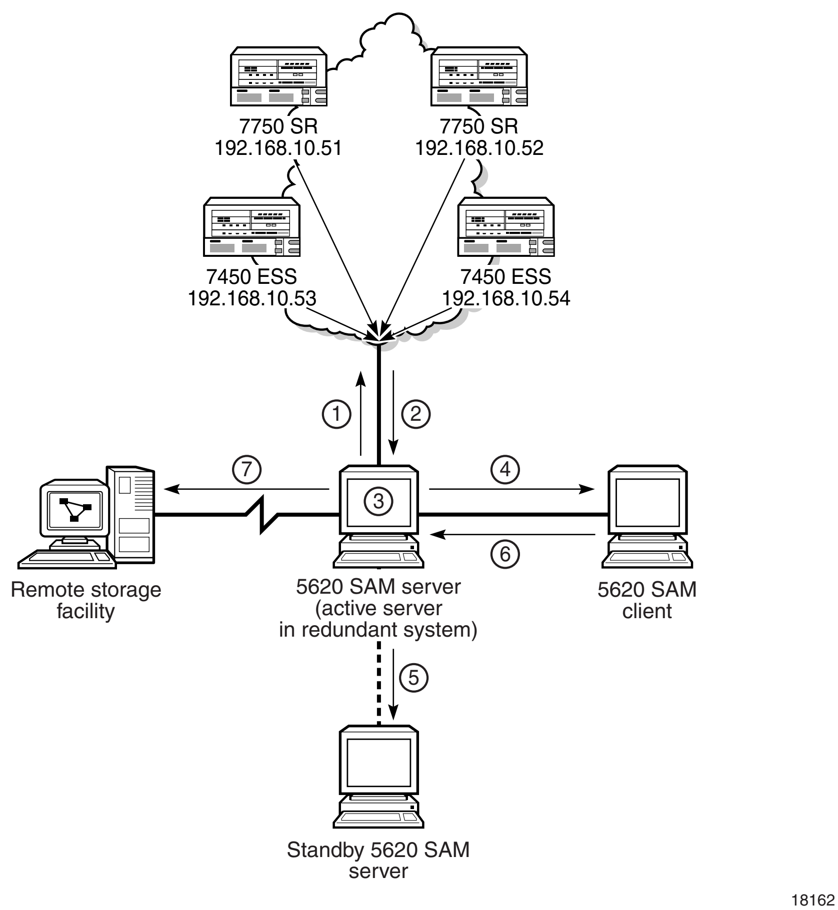


Figure 23-1 illustrates the activities of the 5620 SAM backup/restore process. The labels correspond to events in the following sequence:

1 At the interval specified—every hour in this example—the 5620 SAM issues an FTP or SCP request to all devices for a backup.

2 The devices use FTP or SCP to send the BOF and configuration files to the 5620 SAM server.

3 The 5620 SAM server stores the received files in the 5620 SAM database.

4 An operator using a 5620 SAM client uses the Backup/Restore Status tab of the Backup Policy form to view the backup status.

5 If the 5620 SAM system is a redundant configuration, the active server synchronizes the backed-up information with the standby server.

6 A 5620 SAM operator uses the Backup/Restore form to perform on-demand and scheduled device backups, restores, and configuration saves, as required.

7 A third-party application periodically sends a copy of the backup files from the 5620 SAM server to a remote storage facility for safekeeping.

23.2 Workflow for NE maintenance

1 For secure backups, restores and upgrades, verify that SSH2 is correctly configured on the device and that the 5620 SAM mediation policy for the device is configured for secure FTP or SCP. See chapter 13 for information about device commissioning. See chapter 14 for information about configuring a 5620 SAM mediation policy. Secure backups and upgrades are supported on the following devices:

- 7210 SAS-D 6F 4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6850E
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E

2 Commission the managed devices using a CLI. See chapter 13 for information about device commissioning.

3 Configure the 5620 SAM deployment policy to specify how and when the 5620 SAM tries to send configuration changes from 5620 SAM clients to the managed devices. See Procedure 23-1 for more information.

4 Use the 5620 SAM to configure device backup or restore policies. A device backup policy specifies how often the 5620 SAM backs up the device configuration. See Procedure 23-3 for more information.

As a restore policy works implicitly with a backup, there is no explicit restore policy. The user must select the imported or pre-existing backup file and click on the Restore button.

5 As required, schedule device software upgrades. Scheduled software upgrades are supported on the 7210 SAS-D 6F 4T ETR, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 9500 MPR.

i Create a 5620 SAM schedule. See Procedure 23-18 for more information. See chapter 79 for information about creating 5620 SAM schedules.

ii Create a software upgrade policy and create a 5620 SAM scheduled task for the upgrade activity. See Procedure 23-11 for more information.

iii Review the results and status of the scheduled upgrade and, as required, take the appropriate actions based on your company policies.

iv As required, manage scheduled software upgrades. See Procedure 23-19 for more information.

6 As required, perform on-demand NE configuration saves, backups, and restores.

a Import a device backup file. See Procedure 23-6 for more information.

b Export a device backup file. See Procedure 23-7 for more information.

c Perform an OmniSwitch device backup file. See Procedure 23-8 for more information.

d Restore an OmniSwitch device configuration backup. See Procedure 23-9 for more information.

e Restore a backed up device configuration. See Procedure 23-5 for more information.

7 View the status of various maintenance activities to confirm that scheduled tasks occur as planned.

a View the deployment, backup/restore, or software upgrade status of an NE. See Procedure 23-23 for more information.

b View the accounting statistics collection status of an NE. See Procedure 23-24 for more information.

c View the trap metrics information. See Procedure 23-25 for more information.

8 View the contents of NE file systems by opening an FTP or SSH file browser from the 5620 SAM client GUI, as required. See Procedure 23-26 and Procedure 23-27 for more information.

9 As required, troubleshoot failed configuration deployments using the 5620 SAM alarm window and the Deployment form. See Procedure 23-2 for more information.

23.3 Workflow for a 7450 ESS, 7710 SR, or 7750 SR software upgrade

Caution — Before you perform an ISSU, review the appropriate device release notice for more information about the device software releases that support the ISSU. The software upgrade information in the device documentation takes precedence over this procedure.

1 Perform a preliminary check before you start the software upgrade.

i Manually verify the software image file checksums.

ii Verify that the device supports the new software.

iii Verify that there is sufficient space on the compact flash drive for the software image files.

iv For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

2 Download the software description file to a directory on a 5620 SAM client station.

3 Import the software description file. See Procedure 23-10 for more information.

4 Back up the device configuration. See Procedure 23-4 for more information.

5 Perform a software upgrade to transfer the software image files to each NE that you need to upgrade.

   a Perform a scheduled software upgrade. See Procedure 23-18 for more information.

   b Perform an immediate software upgrade. See Procedure 23-14 for more information.

6 After the upgrade, verify whether the boot environment synchronization is successful.

7 If required, reboot the NE.

Note 1 — Some device software upgrades do not require a reboot; for example, ISA-AA upgrades and ISSUs. See the device documentation for more information.

Note 2 — When you perform an ISSU, you can manually soft reset or hard reboot the IOMs after an upgrade. A soft reset results in minimal downtime, but has restricted support. See Procedure 23-12 for information about a manual soft reset. See Procedure 23-13 for information about a manual hard reboot.

Note 3 — For MDAs, CMAs, and MCMs in a 7710 SR, the device determines what needs to be reset after an ISSU and performs the required resets automatically.

Note 4 — When the IOMs are not manually soft reset or hard rebooted, the device performs a soft reset, if supported, after 2 h; otherwise, the device performs a hard reboot after 2 h.

Note 5 — The 5620 SAM does not support the Reboot Upgrade option on NEs because it is considered too invasive. Such an operation should be performed only through a direct console connection to the NE.

8 View the software upgrade status of the NE to verify whether the upgrade is successful. See Procedure 23-23 for more information.

9 Verify whether the transferred files and configurations are on the device by viewing the contents of the NE file systems through an FTP or SSH file browser, as required. See Procedure 23-26 and Procedure 23-27 for more information.

10 Remove obsolete software images from the device.

11 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 14 for more information.

12 As required, perform upgrade verification tests.

23.4 Workflow for a 7250 SAS software upgrade

Caution — The software upgrade information in the device documentation takes precedence over this procedure. Before you perform a software upgrade, read the device documentation.

1 Perform a preliminary check before you start the software upgrade.

- **i** Verify that the device supports the new software.
- **ii** Verify that there is sufficient space on the compact flash drive for the software image files.

2 Download the software description file to a directory on a 5620 SAM client station.

3 Import the software description file. See Procedure 23-10 for more information.

4 Back up the device configuration using the script manager or CLI.

Note — You cannot use the 5620 SAM to back up or restore the device configuration of the 7250 SAS.

5 Start the upgrade procedure using the script manager. Perform a scheduled software upgrade or an immediate software upgrade to transfer the software image files to each NE that you need to upgrade. Procedure 23-15 for more information about performing an immediate software upgrade. See Procedure 23-18 for more information about performing a scheduled software upgrade.

6 Reboot the NE.

7 View the software upgrade status of the NE to verify whether the upgrade is successful. See Procedure 23-23 for more information.

8 Verify whether the transferred files and configurations are on the device by viewing the contents of the NE file systems through an FTP or SSH file browser, as required. See Procedure 23-26 and Procedure 23-27 for more information.

9 Remove obsolete software images from the device.

10 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 14 for more information.

11 Perform upgrade verification tests, as required.

23.5 Workflow for a 9500 MPR software upgrade

1 Create a 9500 MPR software upgrade policy; see Procedure 23-11 for more information. Configure the FTP server details in the upgrade policy. The images are transferred to the FTP server location and the 9500 MPR node will pickup image files from the configured FTP server.

Note — The software upgrade policy provides the 9500 MPR NE with information about the location of the new software image files during a software upgrade.

2 Download the image package to the 5620 SAM client. Extract the package and ensure that the .DSC file is present in the same folder. When you click on the import button, the 9500 MPR image transfer is initiated, see Procedure 23-10. The image files will be copied and stored temporarily on the 5620 SAM server. When you click on the Upgrade Sites button, the stored image files are transferred to the FTP server and picked up by the 9500 MPR.

Note — The software description files have a .DSC file extension. A software description file identifies the files required to be upgraded to the 9500 MPR.

3 Perform a scheduled software upgrade or an immediate software upgrade to transfer the software image files to each 9500 MPR that you need to upgrade. See Procedure 23-17 for more information about performing an immediate software upgrade. See Procedure 23-18 for more information about performing a scheduled software upgrade.

4 Activate the new software on each upgraded 9500 MPR NE. See Procedure 19-12 for more information about activating software on a 9500 MPR NE.

23.6 NE maintenance procedures

Use the following procedures to perform NE maintenance operations.

Procedure 23-1 To configure the 5620 SAM deployment policy

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Click on the Deployment Policy tab button.

3 Configure the parameters:

- Auto Save Scheme
- Auto Save Threshold
- Scheduled Save Scheme
- Scheduled Save Interval
- Save Details
- Retry Scheme
- Retry Interval
- Retry Threshold

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Deployment form closes.

Procedure 23-2 To troubleshoot a failed configuration deployment

The 5620 SAM continues to retry deployments after a failed or incomplete deployment attempt, based on the 5620 SAM deployment policy, as configured in Procedure 23-1. When there is a deployment error, a number of problems can occur, for example:

- The 5620 SAM database may lose synchronization with the device database.
- Configuration changes requested using the client GUI may clash with configuration changes, retries, and recovery applications developed by an OSS system using the 5620 SAM-O interface or by an operator using a CLI.

When a failed or incomplete deployment or a failed SNMP configuration request occurs, a Problems Encountered error display form appears automatically. This form displays error information about the failure(s).

Note 1 — The Request Id and Task Name fields appearing on the Problems Encountered error form can be used for troubleshooting using the Task Manager application.

Note 2 — The Problems Encountered error form can appear for non-deployment generated errors also.

For example, to view more information on a failed deployment, select a failed deployment entry, then click on the Properties button, or double-click on the failed deployment entry.

An error form opens which contains a View Affected Object button and a Details button.

Click on the Details button to view detailed diagnostic information about the failure(s).

Click on the View Affected Object button. A form displaying object properties opens. This form facilitates rapid navigation to the object which caused the failure for troubleshooting purposes.

Click on the Faults tab button. Alarm information related to the failure(s) is displayed.

A failure error message is not generated when the alarm is cleared or the failure entry is deleted.

Note 1 — If a deployment failure is associated with more than one 5620 SAM GUI, the Problems Encountered form and related forms appear only on the GUI from which the deployment was issued.

Note 2 — The automatically generated Problems Encountered form and related forms, are an additional tool to the following troubleshooting procedure.

The Deployment form displays failed configuration deployments and allows you to view information about failed deployments. Using this form, you can clear the deployment, override the error to force the configuration to be downloaded to the device, or suspend or resume deployment retries to a device.

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Review the deployment information. The State value indicates the cause of the deployment failure.

3 Select a deployment in the list and click on the Properties button. The properties form for the deployment opens. The objects that the deployment failed to modify are displayed in the Objects list.

4 Select an entry in the Objects list and click on the Properties button. The Object Change form that describes the attempted configuration change opens.

5 Select an entry in the Attributes list and click on the Properties button. The Attribute Change form opens and displays the following object attribute information for troubleshooting:

- the NE attribute that was to be modified
- the old, unmodified attribute value
- the new attribute value that the deployment failed to assign

6 Click on the Cancel button to close the Attribute Change form.

7 Click on the Cancel button to close the Object Change form.

8 Click on the Cancel button to close the deployment properties form.

9 Perform one of the following actions, depending on the result of the investigation into the failed deployment.

a Click on the Suspend Retries button to override the deployment policy setting and prevent further retries of the deployment. A dialog box appears; click on the Yes button.

b Click on the Resume Retries button to override a previous Suspend Retries action performed on the deployment. A dialog box appears; click on the Yes button.

c Click on the Clear button to clear the deployment. A dialog box appears; click on the Yes button. The deployment is cleared.

Note — Clearing a failed deployment may result in a loss of data synchronization between the 5620 SAM database and the NE. Alcatel-Lucent recommends that you resynchronize the NE objects associated with a failed deployment after you clear a failed NE deployment.

d Click on the Force Submit button to force the 5620 SAM to immediately resend the deployment to the NE. A dialog box appears; click on the Yes button.

10 Click on the Refresh button to update the list of failed deployments.

11 Take the appropriate action described in this procedure to troubleshoot other failed deployments, as required.

12 Close the Deployment form.

Procedure 23-3 To create a device backup policy

Perform this procedure to create a device backup policy and assign it to NEs.

Note — The default backup policy is assigned automatically to all 5620 SAM-managed NEs that do not currently have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Create button. The Backup Policy (Create) form opens.

3 Specify whether backup functionality is enabled.

a Enable the Enable Backup parameter.

b Disable the Enable Backup parameter. The remaining parameters on the form cannot be configured. Go to step 13.

4 Configure the following parameters:

- Policy ID
- Auto-Assign ID
- Name
- Policy Type

5 If you selected AOS Based Node policy type, go to step 7.

6 Specify whether to perform a reboot after the configuration is restored to the device by specifying the Auto-Reboot After Successful Activation parameter.

Caution — When you use the 5620 SAM client GUI to restore a managed device configuration and you disable the Auto-Reboot After Successful Activation parameter, there is a risk that the bof.cfg file may be overwritten in the following situations:

- when a user performs “bof save” using CLI on the managed device
- If there is a gap between a restore and a reboot, perform a “show bof” to ensure that another user has not performed a “bof save”.

7 You can schedule backups based on a time interval or on the number of NE configurations performed from the 5620 SAM server. Configure the backup triggering parameters:

- Scheduled Backup Scheme
- Scheduled Backup Interval
- Scheduled Backup Sync Time
- Scheduled Backup Threshold (operations)
- Auto Backup Scheme
- Auto Backup Threshold (operations)

8 Perform one of the following:

a If you selected SR Based Node policy type, go to step 9.

b If you selected AOS Based Node policy type, go to step 11.

c If you selected MPR Based Node policy type, go to step 12.

Note 1 — See the *5620 SAM LTE RAN User Guide* for more information on creating a backup policy for an eNodeB.

Note 2 — See the *5620 SAM Optical User Guide* for more information on creating a backup policy for an 1830 PSS.

Note 3 — See the *5620 SAM LTE ePC User Guide* for more information on creating a backup policy for a 7750 MG.

9 Configure the Backup Settings parameters:

- CLI Config File Mode
- CLI Config Save Details
- CLI Debug Save Config File Mode
- Boot Option File Mode
- File Compression

Note — In addition to enabling the CLI Debug Save Config File Mode parameter, you must specify the location of the debug configuration files in the 5620 SAM main server configuration. See chapter 6 for information about how to specify the location of the debug configuration files in the main server configuration.

10 Go to step 12.

11 Configure the AOS Backup Settings parameters:

- Save Certified Directory
- Save Network Directory
- File Compression

Note — The 5620 SAM can only backup configuration files stored in the certified directory. If you need to backup configuration files in the working directory, you must ensure that the files in the certified and working directories are identical. See Procedure 19-13 to perform a Certify or Certify and Synchro command before you backup the OmniSwitch configuration files.

12 Configure the parameters in the Backup Purging panel. Backup purging parameters allow you to specify the number of backup files kept. These settings allow you to eliminate manual monitoring and deletion of backup files. The purge criteria can be the number of files, the age of the files, or both.

- Auto-Purge Scheme
- Number of Backups
- Maximum Backup Age (days)

13 Click on the OK button to save the backup policy. The Backup Policy (Create) form closes.

14 Assign the policy to NEs as required.

i Select the new policy in the list and click on the Properties button. The Backup Policy (Edit) form opens.

ii Click on the Backup/Restore Policy Assignment tab button. The Backup Policy (Edit) Filter form opens.

iii Configure an advanced search, if required. See Procedure 3-27 for more information.

iv Click on the OK button. The Backup Policy (Edit) Filter form closes and the filtered NEs appear in the Unassigned Sites or Assigned Sites lists.

v Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.

vi Click on the OK button. The Backup Policy (Edit) form closes and a dialog box appears.

vii Click on the Yes button. The policy is assigned to the NEs.

15 The 5620 SAM creates the backup based on the specified schedule.

You can optionally perform the backup immediately. See Procedure 23-4 for more information.

16 Close the Backup/Restore form.

Procedure 23-4 To perform an immediate device backup, restore, or configuration save

When you start an immediate backup, you back up the device configuration based on the backup policy associated with the NE.

A device configuration restore operation uses the most recently backed-up device configuration file unless otherwise specified. See Procedure 23-5 for more information.

The following conditions must be present before you can perform a device configuration backup, restore, or configuration save:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 9 for more information about scope of command roles.
- FTP or secure FTP is configured in the mediation policy for the NE. See chapter 14 for more information.
- The BOF persist parameter is set on the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, 7710 SR, and 7750 SR. See chapter 13 for information about device commissioning.

Depending on the operation type, the Backup State or Restore State column displays the current state of the operation. The possible values are:

- Not Attempted - the operation is unattempted
- Saving Config - the device configuration is being saved on the device
- Transferring Files - a file transfer is in progress
- Success - the operation is complete and successful
- Failure - the operation is complete but unsuccessful
- CPM Sync and Pending Reboot - the device configuration is restored and the device is synchronizing the CPMs before it reboots
- CPM Sync and Pending Reboot Standby - the 5620 SAM is waiting for the reboot of the standby CPM
- Standby Reboot and Pending Redundant Switch-over - the 5620 SAM is waiting for the switchover to the standby CPM

Note — During a backup, if a device is unresponsive to the 5620 SAM because SNMP on the device is disabled, the Backup State column entry for the device does not immediately display the correct value of Failed. This latency is caused by the inability of the 5620 SAM to communicate with the unresponsive device. In such a situation, the Backup State column displays the initial value of Saving Config until three 10-minute SNMP polling periods, or 30 minutes, have elapsed, after which the Backup State changes to Failed if SNMP remains disabled.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2 Click on the Backup/Restore Status tab button. The managed devices are listed.

3 Select a device from the list and click on the Backup button, the Restore button, or the Save Config button, depending on the operation that you want to perform. A dialog box appears.

4 Click on the Yes button. The backup or restore operation starts, and the current backup or restore state for the device is indicated in the Backup State or Restore State column.

5 You can resynchronize an NE with the 5620 SAM database, if required, by clicking on the Resync button. See chapter 14 for information about resynchronizing an NE.

6 Close the Backup/Restore form.

Procedure 23-5 To restore a device configuration backup other than the most recent

You can choose to restore an older version of the device configuration to meet special network requirements.

Caution 1 — Older backups do not have the most recent network information. Restoring an older device configuration may be service-affecting.

Caution 2 — Ensure that you back up the current device configuration using Procedure 23-3 before you proceed.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The Backup/Restore form opens.

2 Click on the Backup/Restore Status tab. The managed devices are listed.

3 Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.

4 Click on the Backups tab button. A list of configuration backups for the selected device opens, ordered from the oldest to the most recent.

5 Select a backup in the list and click on the Restore button. A dialog box appears.

6 Click on the Yes button.

7 Click on the Resync button to ensure the latest network information is available, if required.

8 Close the Backup/Restore form.

Procedure 23-6 To import a device backup to the 5620 SAM database

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab button.

3 Select the NE in the list for which you are importing a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the More Actions button and choose Import. A file navigator form opens.

5 Use the form to specify the directory that contains the device backup and click on the OK button.

If the directory contains a backup for this NE, the 5620 SAM imports the backup files into the 5620 SAM database and the import is successful. Otherwise, a dialog box appears if the directory does not contain a backup from this NE, and the import fails. Click on the OK button to close the dialog box.

6 Close the NE Backup/Restore Status form.

7 Close the Backup/Restore form.

Procedure 23-7 To export a device backup to a file

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab button.

3 Select the NE in the list for which you are exporting a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the Backups tab button. A list of backups for the NE is displayed.

5 Select a backup in the list and click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported device backup and click on the OK button. The NE configuration backup is saved to the specified directory.

7 Close the NE Backup/Restore Status form.

8 Close the Backup/Restore form.

Procedure 23-8 To perform a device backup on an OmniSwitch

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch icon, right-click on an OmniSwitch shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Software Control Module tab button. Ensure the Running Directory field value is Working.

4 Ensure the Certified Status field value is Certified. If the value is not Certified, click on the drop down menu in the Command to Apply field. Choose Certified. Click on the Apply button. A dialog box appears. Click on the Yes button. The Certified Status field value changes to Certified.

Note — It is necessary to do a Resync to make sure the "/flash/working" and "/flash/certified" directories are the same even though the Certified Status field is shown as Certified. Go to Step 5.

5 Click on the Resync button. A dialog box appears. Click on the Yes button.

6 Perform an NE backup by choosing Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The BackupRestore form opens in the Backup/Restore Policy tab. Click on the Backup/Restore Status tab button. A list of all the backup files associated with a backup policy appears. See Procedure 23-3 for details.

7 Export a copy of the backup onto a local drive.

Procedure 23-9 To restore a configuration backup on an OmniSwitch

First, perform an OmniSwitch device backup, using Procedure 23-8.

Note — To restore an OmniSwitch NE's configuration files, by performing Procedure 23-8, a backup file located in the 5620 SAM database is created. Therefore, a Backup/ Restore Policy will already exist in the 5620 SAM database.

1 On the BackupRestore form, choose the OmniSwitch NE on which you want to perform the restore. Click on the Properties button. The NE Backup/Restore Status details form opens for that NE. Click on the Backups tab button. Choose the file you want to restore.

Note — You can import the locally available backup file for the same NE to the 5620 SAM which can be restored. Ensure the backup policy remains the same as was in place during the backup procedure. This will prevent the 5620 SAM throwing an error while importing the file.

2 A Confirm dialog box appears. Click on the Yes button.

3 With the appropriate OmniSwitch file chosen, click on the Properties button. The NE BackupRestore Status - AOS Policy form appears. The Restore Status panel indicates Restore Time, Restore State and last Successful Restore Time values.

Note 1 — The restored back-up configuration is stored on a working directory.

Note 2 — The restored back-up configuration is stored on a working directory. Success indicates that the file has been successfully transferred to the appropriate NEs. However, the file will not become active until the device(s) have been reloaded from working.

4 Right-click on an OmniSwitch shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

5 Click on the Software Control Module tab button. Click on the drop down menu in the Command to Apply field. Choose Reload from Working.

6 Click on the Apply button. A dialog box appears. Click on the Yes button.

7 If required, configure the Delayed Activation Timer parameter.

8 In order to certify the restored configurations, ensure the Certified Status field value is Certified, after validating all the data. See Step 4 of Procedure 23-8.

Procedure 23-10 To import device software image or description files to the 5620 SAM database

Perform this procedure to import a set of device software files or 9500 MPR software description files into the 5620 SAM database for use during device software upgrades.

1 Make the new device software files available to the 5620 SAM.

i If the device software files are compressed in an archive, for example, a TiMOS ZIP file, extract the files from the archive.

Note — Depending on the device type and version, the compressed files in a device software archive do not extract to a flat directory structure.

ii Copy or move the files to a directory that is accessible to the 5620 SAM.

Note 1 — The directory must contain a valid and complete set of device software files, and must not contain other files or subdirectories.

Note 2 — Alcatel-Lucent recommends that all OmniSwitch software image files, including any optional and boot files, are available in the specified directory for importing to the 5620 SAM database.

Note 3 — 9500 MPR NEs require only the software description (.DSC) files to be available for importing into the 5620 SAM database.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Click on the Software Images tab button.

4 Click on the appropriate tab button for the type of NE that you need to upgrade.

5 Click on the Import button. The Open window appears.

6 Navigate to directory that contains the software image, select the image, and click on the Open button. The software image appears in the list.

Note — You upgrade a Release 8.0 R1 or later 7450 ESS, 7710 SR, or 7750 SR using a common software image. The Product Name field displays Alcatel-SR/ESS-7XXX to indicate that the software image is a common software image.

The 5620 SAM verifies that only the required files are present and then imports the files from the specified directory into the 5620 SAM database. An entry for the image appears in the list.

If the directory does not contain only the required files, a dialog box appears. Go to step 7. Otherwise, go to step 8.

7 Perform the following:

  i Click on the OK button.

  ii Copy or move files, as required, to ensure that the directory contains only the files required for the upgrade.

  iii Go to step 5.

8 Close the Software Upgrade form.

Procedure 23-11 To create a software upgrade policy

Perform this procedure to create a policy that can be used to perform an immediate or scheduled device software image upgrade. Contact your Alcatel-Lucent technical support representative for information about downgrades.

You cannot create a software upgrade policy on the 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, or 7210 SAS-M 24F 2XFP ETR.

1 Perform Procedure 23-10 to import the required device software image.

2 Ensure that the following conditions are present.

- Appropriate FTP accounts are configured and available on the devices.
- The device configuration files are backed up, as described in Procedures 23-3 and 23-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Click on the Create button. The Software Upgrade Policy (Create) form opens.

5 Configure the Policy Type parameter.

6 Perform one of the following.

  a If you selected SR Based Node in step 5, go to step 7.

  b If you selected AOS Based Node in step 5, go to step 10.

  c If you selected MPR Node in step 5, go to step 12.

Note 1 — See the *5620 SAM LTE ePC User Guide* for more information about 9471 MME and 7750 MG software file transfers and software upgrades.

Note 2 — See the *5620 SAM LTE RAN User Guide* for more information about eNodeB software upgrades.

7 Configure the following parameters:

- Auto-Assign ID
- Policy ID
- Name
- CFlash Image Root Path
- CFlash Backup Root Path

Note 1 — You can open an FTP or SSH file browser from this form to determine the values to use for the CFlash Image Root Path and CFlash Backup Root Path parameters. Click on the More Actions button and choose FTP File Browser or SSH File Browser, as required. See Procedures 23-26 and 23-27 for more information.

Note 2 — By default, compact flash cf3 is used to store image and backup files. Some NE types do not support a cf3, for example the 7210 SAS supports only one compact flash designated as cf1. Ensure that you specify a supported compact flash for the NE type when you configure the CFlash Image Root Path and CFlash Backup Root Path parameters.

8 Perform one of the following actions, as required.

a To specify an out-of-service upgrade that activates the new software image after the download but does not reboot the NE, enable the Auto-Activate After Successful File Transfer parameter and ensure that the Auto-Reboot After Successful Activation parameter is disabled.

Note 1 — You are not required to reboot for some NE software upgrades; for example ISA-AA upgrades. See the associated node documentation for additional information.

Note 2 — The 5620 SAM does not support the Reboot Upgrade option on NEs because it is considered too invasive. Such an operation should be performed only through a direct console connection to the NE.

b To specify an out-of-service upgrade that includes rebooting the NE after activating the software, enable the Auto-Reboot After Successful Activation parameter. When you are downloading multiple images to multiple devices, Alcatel-Lucent recommends that you disable the Auto-Reboot After Successful Upgrade option to ensure that the new software properly transfers.

When you enable the Auto-Reboot After Successful Activation parameter, you are prompted to acknowledge the action because it is potentially service-affecting. Before you proceed, ensure that you understand the implications of automatically rebooting the NE after an upgrade.

The Auto-Reboot After Successful Activation parameter is configurable when the In Service Software Upgrade parameter is disabled.

Caution — When you use the 5620 SAM client GUI to perform a managed device software upgrade and you disable the Auto-Activate After Successful File Transfer and Auto-Reboot After Successful Activation parameters, there is a risk that the bof.cfg file may be overwritten in these situations:

- if a user performs ‘bof save’ using CLI on the managed device
- if there is a gap between the software upgrade and the reboot

Perform a ‘show bof’ to verify that the BOF has not been overwritten.

c To specify an in-service upgrade, select In Service Software Upgrade to upgrade a device with dual CPMs.

Note 1 — An in-service software upgrade is not supported between every maintenance and major release. For upgrades that do not support in-service software upgrades, you must perform an out-of-service upgrade. Refer to the appropriate network element documentation for supported in-service upgrade release transitions.

Note 2 — Specifying an in-service software upgrade disables the Auto-Reboot After Successful Activation parameter.

9 Go to step 13.

10 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Image Root Path
- Upgrade File Type

11 Go to step 13.

12 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- FTP User ID
- FTP Password
- FTP Server IP
- FTP Server Port
- Root Directory
- Forced Download
- Auto-Activate After Successful File Transfer

13 Click on the Apply button. The Software Upgrade Policy (Create) form refreshes with additional tab buttons and the form name changes to Software Upgrade Policy (Edit).

14 Assign the policy to NEs as required.

- **i** Click on the Software Upgrade Policy Assignment tab button. The Software Upgrade Policy Filter (edit) form opens.
- **ii** Configure the filter parameters, if required. Click on the OK button.
- **iii** Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.
- **iv** Click on the OK button. A dialog box appears.
- **v** Click on the Yes button. The policy is assigned to the NEs.

15 Close the Software Upgrade Policy (Edit) form. The new policy is displayed on the Software Upgrade form.

Procedure 23-12 To perform a soft reset of an IOM or IMM

Use this procedure to perform a manual soft reset of one of the following:

- an IOM in a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, or 7750 SR
- an IOM3 or IMM in a Release 8.0 R1 or later 7450 ESS or 7750 SR

Note — Soft reset is supported only under the following conditions:

- The IOM is operationally up.
- The IOM is supported.
- The MDAs are Ethernet MDAs but not HSMDAs, and are provisioned.

1 To select the IOM, choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the an NE and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the card slot level, right-click on the card slot and select Soft Reset from the contextual menu. A Warning form opens.

5 View the dependency information.

6 Select the I understand the implications of this action check box.

7 Click on the Yes button. The operational state of the IO card displays the soft reset status when the soft reset is in progress.

Procedure 23-13 To perform a hard reboot of an IOM

Use this procedure to perform a manual hard reboot of an IOM.

1 To select the IOM, choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the an NE and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the card slot level and click on the card slot. The Card Slot form opens.

5 Click on the IO Card tab button.

6 Click on the More Actions button and choose Reboot. The operational state of the IO card displays the hard reboot status when the hard reboot is in progress.

7 Close the Card Slot form.

Procedure 23-14 To perform an immediate software upgrade on a 7450 ESS, 7710 SR, or 7750 SR

The following conditions must be true before you attempt a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 9 for more information about scope of command roles.
- The FTP or secure FTP must be configured in the mediation policy for the NE. See chapter 14 for more information.

Warning — Devices, such as the 7450 ESS and 7750 SR, may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility and about the firmware upgrade procedures.

Caution 1 — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device if the upgrade fails.

Caution 2 — Before you perform a software upgrade, read the device documentation. The software upgrade information in the device documentation takes precedence over this procedure.

Caution 3 — Before you perform an ISSU, review the appropriate device release notice for more information about the device software releases that support the ISSU. See section 23.1 for more information about the ISSU.

Note — If you downgrade a device software image, you must unmanage and delete the device before you perform the downgrade, as described in Procedure 14-13. Contact your Alcatel-Lucent technical support representative for information about downgrades.

1 Perform a preliminary check before you start the software upgrade.

- **i** Manually verify the software image file checksums.
- **ii** Verify that the device supports the new software.
- **iii** Verify that the compact flash drive has sufficient space for the software image files.
- **iv** For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

2 Back up the device configuration. See Procedure 23-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs an upgrade on each NE to which the software upgrade policy is assigned and performs each upgrade according to the policy configuration.

5 Click on the Software Images tab button.

6 Choose a software image in the list and click on the Import button. The Open window appears.

7 Navigate to the directory that contains the software image, select the image, and click on the Open button.

Note — You upgrade a Release 8.0 R1 or later 7450 ESS, 7710 SR, or 7750 SR using a common software image. The Product Name field displays Alcatel-SR/ESS-7XXX to indicate that the software image is a common software image.

The 5620 SAM verifies that only the required files for the upgrade are present and then imports the files from the specified directory into the 5620 SAM database. An entry for the image appears in the list.

If the directory does not contain only the required files, a dialog box appears. Go to step 8. Otherwise, go to step 9.

8 Perform the following:

i Click on the OK button.

ii Copy or move files to ensure that the directory contains only the files required for the upgrade.

iii Go to step 6.

9 Click on the Upgrade Sites button. A list of NEs appears. The list is filtered to display only the device type that is appropriate for the specified software image.

Note — If you select a common software image in step 7, only the 7450 ESS, 7750 SR, and 7710 SR devices are listed.

10 Choose one or more NEs in the list.

11 Click on the OK button. The software upgrade starts.

12 Click on the Software Upgrade Status tab button to view the progress of the upgrade.

13 Reboot the NE if the Auto-Reboot After Successful Activation parameter is disabled in the software upgrade policy. Perform one of the following actions.

Note 1 — Some device software upgrades do not require a reboot; for example, ISA-AA upgrades and ISSUs. See the device documentation for more information.

Note 2 — When you perform an ISSU, you can manually soft reset or hard reboot the IOMs or IMMs after an upgrade. A soft reset results in minimal downtime, but has restricted support. See Procedure 23-12 to perform a manual soft reset, or Procedure 23-13 to perform a manual hard reboot.

Note 3 — For MDAs, CMAs, and MCMs in a 7710 SR, the device performs the required resets automatically after an ISSU.

Note 4 — When the IOMs are not manually soft reset or hard rebooted, the device performs a soft reset, if supported, after 2 h; otherwise, the device performs a hard reboot after 2 h.

Note 5 — The 5620 SAM does not support the Reboot Upgrade option on NEs because it is considered too invasive. Such an operation should be performed only through a direct console connection to the NE.

a Use a Telnet or SSH CLI session.

i Right-click on the NE and choose NE Session→Telnet Session or NE Session→SSH Session.

ii Enter the following at the command prompt:

`admin reboot now` ↵

The NE reboots.

b Use the 5620 SAM GUI.

i Choose Equipment from the 5620 SAM navigation tree drop-down menu.

ii Navigate to the NE shelf object. The path is Routing→NE→Shelf.

iii Right-click on the shelf object and choose Reboot. The NE reboots.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a scheduled maintenance window.

14 Verify whether the upgrade is successful, as described in Procedure 23-23.

15 Use the FTP or SSH file browser to verify whether the transferred files and configurations are on the managed device. See Procedure 23-26 for information about using an FTP file browser. See Procedure 23-27 for information about using an SSH file browser.

16 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 14 for information about resynchronizing an NE.

17 Perform upgrade verification tests, as required.

Procedure 23-15 To perform an immediate software upgrade on a 7250 SAS

The following conditions must be true before you attempt a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 9 for more information about scope of command roles.
- The FTP or secure FTP must be configured in the mediation policy for the NE. See chapter 14 for more information.

Caution 1 — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device in the event of an upgrade failure.

Caution 2 — Before you perform a software upgrade, read the device documentation. The software upgrade information in the device documentation takes precedence over this procedure.

Note — If you downgrade a device software image, you must unmanage and delete the device before you perform the downgrade, as described in Procedure 14-13. Contact your Alcatel-Lucent technical support representative for information about downgrades.

1 Perform a preliminary check before you begin the software upgrade.

i Verify that the device supports the new software.

ii Verify that the compact flash drive has sufficient space for the software image files.

2 Download the software description file to a directory on a 5620 SAM client station.

3 Load the software description file from step 2 into the TFTP server. See Procedure 23-10 for more information.

4 Back up the device configuration using the 5620 SAM Script Manager.

5 Start the upgrade procedure using the 5620 SAM Script Manager. Code 23-1 is an example of an upgrade script.

Code 23-1: 7250 SAS upgrade script example

```
#*
<velocityProperties>
```

```
  <tab><name>BiNOS Upgrade</name><tooltip>BiNOS Upgrade
Info</tooltip>
    <group><name>BiNOS Version</name><tooltip>BiNOS
Version</tooltip>
      <uiOrder>0</uiOrder>
      <property>
        <name>binos_version</name>
        <uiName>BiNOS Version:</uiName>
        <type>ComboBox</type>
        <default>BiNOS-7250-ES_v2_0_R7.0.Z</default>
        <uiOrder>0</uiOrder>
        <list>
          <item><name>BiNOS 7250ES Release
2.0-R5.2</name><value>BiNOS-7250-ES_v2_0_R5.2.Z</value></item>
          <item><name>BiNOS 7250ES Release
2.0-R6.1</name><value>BiNOS-7250-ES_v2_0_R6.1.Z</value></item>
          <item><name>BiNOS 7250ES Release
2.0-R7.0</name><value>BiNOS-7250-ES_v2_0_R7.0.Z</value></item>
        </list><tooltip>BiNOS Version</tooltip>
        <runtime>true</runtime>
      </property>
    </group>
  </tab>
</velocityProperties>
*#
config boot
   application $binos_version
   device local
   exit
dir Boot
config boot
   show
   exit
```

6 Reboot the NE.

7 Verify whether the upgrade is successful, as described in Procedure 23-23.

8 Use the FTP or SSH file browser to verify that the transferred files and configurations are on the device. See Procedure 23-26 for information about using an FTP file browser. See Procedure 23-27 for information about using an SSH file browser.

9 Remove obsolete software images from the device.

10 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 14 for information about resynchronizing an NE.

11 Perform upgrade verification tests, as required.

Procedure 23-16 To perform an immediate software upgrade on an OmniSwitch

The directory structure that stores the image and configuration files is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default files for the switch.
- The working directory contains files that may or may not be modified from the certified directory. The working directory is a holding place for new files. Files in the working directory must be tested before you commit them to the certified directory.

The following conditions must be present before you can perform a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 9 for more information about scope of command roles.
- FTP is configured in the mediation policy for the NE. See chapter 14 for more information.

Warning — An OmniSwitch may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility.

Caution — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device in the event of an upgrade failure.

Perform the following procedure to perform an immediate software upgrade of an OmniSwitch. You can perform the following types of software upgrades:

- Image file
- Boot files
- FPGA files (OS 6855 only)

Note 1 — To perform an ISSU, which is supported only on the OS 9700E and OS 9800E, Release 6.4.2 R1, use the software upgrade window only.

Note 2 — The OS 9700E and OS 9800E NEs support standard software upgrades as described above, in addition to ISSU, with CMM images running on these NEs, and with minimal interruption of data traffic. Currently on OmniSwitch systems the introduction of new images necessitates a system reload which disrupts all data traffic during the reload process. As is the case for a CMM Takeover on current OS 9700E and OS 9800E based systems, data traffic loss should be limited to Layer 3 base traffic and no loss of Layer 2 data traffic should occur. Standard procedures can be used for a normal upgrade or an ISSU.

Note 3 — The operational restrictions and requirements are:

- Only OS 9700E and OS 9800E NEs CMM images have the ability to be upgraded.
- The following CMM images are ISSU capable: Jbase.img, Jsecu.img, Jadvrout.img and Jos.img.
- The OS 9700E and OS 9800E NE platforms must bet fully synchronized and certified.
- Target images must be loaded to the /flash/issu directory.
- Sufficient flash memory must be available for upgrade images.
- The CMM software build must be in the same major build tree branch, differing only in the build number (6.4.1.*.R01)
- NEs running an 'R##' build, such as 6.4.1.123.R01 do not support ISSU patches. The NE must first be upgraded to an 'S##' build such as 6.4.1.123.S01.

See Procedure 23-14 to perform an immediate software upgrade on a SR or ESS NE.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Perform one of the following:

a If you need to upgrade the image files or the image and boot files, go to step 3.

b If you need to upgrade the boot files, go to step 18.

c If you need to upgrade the FPGA files, go to step 32.

3 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab button.

5 Click on the AOS Software tab button.

6 Choose a software image in the list.

7 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

8 Choose one or more NEs in the list.

9 Click on the OK button. The selected software image file is uploaded to the working directory of the selected NEs.

10 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 11.

11 Click on the Reload working Sites button. A list of NEs opens.

12 Choose one or more NEs in the list.

13 Click on the OK button. The selected NEs reboots using the new software image that was uploaded to the working directory.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

Note — Alcatel-Lucent recommends monitoring the switch to ensure that the reboot completes successfully.

14 Click on the Certify Sites button. A list of NEs opens.

Note — Only software that has been thoroughly validated as viable and reliable software should be copied to the certified directory. After you copy the software to the certified directory, you cannot recover a previous version of the image or configuration files.

15 Choose one or more NEs in the list.

16 Click on the OK button. The software image stored in the NE working directory is copied to the certified directory. The working directory and the certified directory are synchronized so that the same files are in both directories.

17 Perform one of the following:

- **a** If you need to upgrade the boot files, go to step 26.
- **b** If you need to upgrade the FPGA files, go to step 34.
- **c** If you are only upgrading the image files, go to step 39.

18 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

19 Click on the Software Images tab button.

20 Click on the AOS Software tab button.

21 Choose a software image in the list.

22 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

23 Choose one or more NEs in the list.

24 Click on the OK button. The boot files are uploaded to the root directory of the selected NEs.

25 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 26.

26 Click on the Upgrade Boot files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected files.

27 Choose one or more NEs in the list.

28 Click on the OK button. The boot files are upgraded on the selected NEs.

29 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 30.

30 Click on the Delete boot files button.

31 Perform one of the following:

- **a** If you need to upgrade the FPGA files, go to step 34.
- **b** If you do not need to upgrade the FPGA files, go to step 39.

32 Click on the Software Images tab button.

33 Click on the AOS Software tab button.

34 Choose a software image in the list.

35 Click on the Upgrade FPGA files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected file type.

36 Choose one or more NEs in the list.

37 Click on the OK button. The selected FPGA files are uploaded to the root directory of the selected NEs.

38 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. After the FPGA files are successfully transferred, the selected NEs are rebooted.

39 Verify the upgrade success, as described in Procedure 23-23.

40 Close the Software Upgrade form.

Procedure 23-17 To perform an immediate software upgrade on a 9500 MPR

Perform the following procedure to download 9500 MPR software to one or more 9500 MPRs. After a successful software upgrade, perform Procedure 19-12 to activate the software on the 9500 MPR NE.

The 9500 MPR software is stored in two banks on a compact flash card:

- The committed bank contains the software that is currently running.
- The standby bank contains downloaded software that has not been activated or software that was active before the current committed software.

Note — A 9500 MPR that has never been upgraded only displays the committed bank. The standby bank does not appear until new software is downloaded for the first time.

You need a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package before you can perform a 9500 MPR software download. See chapter 9 for more information about scope of command roles.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

3 Click on the Software Images tab button.

4 Click on the MPR 9500 Software Images tab button.

5 Choose a software image file in the list. The image descriptor file has a .DSC file extension and must be present on the client system. Other software files do not need to be present on the client system.

6 Click on the Upgrade Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

7 Choose one or more NEs in the list.

8 Click on the OK button. The software upgrade starts.

9 Click on the Software Upgrade Status tab button to view the status of the upgrade as it progresses. Verify that the files are successfully transferred before you go to step 10.

Note — If the Auto-Activate After Successful File Transfer check box is enabled, the device activates the new software image after an upgrade operation successfully completes.

10 Close the Software Upgrade form.

Procedure 23-18 To schedule a software upgrade

Perform this procedure to schedule a device software upgrade on one or more managed NEs according to a software upgrade policy and a 5620 SAM schedule. See Procedure 23-14 for information about creating a software upgrade policy. See chapter 79 for information about creating schedules.

Note — A new SAM scheduled task is shut down by default and must be turned up before it can be executed with one exception. Scheduled software upgrade tasks associated with all NE types are by default auto-enabled.

1 Perform Procedure 23-10 to import the required device software image.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Select the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab button.

5 Select a software image in the list and click on the Schedule Upgrades button. The Select Sites form opens.

6 Choose an NE in the list and click on the OK button. You can choose multiple NEs. The Select Schedule form opens.

Note 1 — If no schedules are listed, you can create one for the upgrade. You cannot proceed unless a schedule is available. See chapter 79 for information about creating 5620 SAM schedules.

Note 2 — You cannot use a schedule in which the Ongoing parameter is enabled.

7 Select a schedule in the list and click on the OK button. See Procedure 23-19 and chapter 79 for more information on how to create a schedule. A dialog box appears.

8 Click on the Yes button. The 5620 SAM schedules the upgrade.

9 Close the Software Upgrade form.

Procedure 23-19 To manage scheduled software upgrades

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab button.

3 Click on the Scheduled Task button. The Scheduled Task form opens.

4 Configure the filter criteria and click on the Search button. A list of scheduled tasks is displayed.

5 Choose a scheduled software upgrade entry.

6 To view the scheduled task configuration, click on the Properties button. The Software Upgrade Scheduled Task form opens.

7 Administratively enable or disable the scheduled software upgrade, if required, by configuring the Administrative State parameter.

8 Click on the Properties button in the Schedule panel to view the schedule information, if required.

9 Click on the Properties button in the Task panel to view the 5620 SAM task information, if required.

10 Close the Software Upgrade Scheduled Task form. The Scheduled Task form reappears.

11 Click on the Task Action button and choose the appropriate option to turn up, shut down, or execute the task, if required.

12 Click on the Delete button to remove the scheduled task from the 5620 SAM, if required.

Note 1 — You cannot delete a scheduled task that is operationally enabled. Click on the Task Action button and choose Shut Down from the menu to operationally disable the scheduled task before you delete it.

Note 2 — The 5620 SAM does not delete a scheduled task after it runs; you must delete it manually. You cannot reuse a completed scheduled task.

13 Close the Scheduled Task form. The Software Upgrade form reappears.

14 Close the Software Upgrade form.

Procedure 23-20 To monitor software upgrade status

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Click on the Software Upgrade Status tab button.

3 Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.

4 Select an NE from the list and click on the Properties button. The Software Upgrade Status (View) form opens.

5 Click on the Software Upgrade tab to view information on the software upgrade.

6 Close the Software Upgrade Status (View) form.

7 Close the Software Upgrade form.

Procedure 23-21 To activate a device software image

Perform this procedure to activate a previously downloaded device software image on an NE. When the 5620 SAM activates an NE software image, it does the following:

- Updates the BOF with the new software image location
- Backs up the original boot.ldr at the location specified by the CFlash Backup Root Path parameter

- Replaces the currently active boot.ldr file with the new one
- Forces a “boot env synch” and a “config synch” on NEs that have redundant CPMs

Note 1 — If the BOF update fails, then the original boot.ldr file is put in place to align with the BOF specification.

Note 2 — The 5620 SAM ensures that the software image is present on the NE and valid for the device before it updates the BOF.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab button. A list of NEs is displayed.

3 Choose an NE in the list.

4 Click on the Software Images tab button. A list of software images on the selected NE is displayed.

5 Select a software image in the list and click on the Activate button. A dialog box appears.

6 Click on the Yes button. The software image is activated.

7 Verify the activation success, as described in Procedure 23-23.

8 Close the Software Upgrade form.

Procedure 23-22 To export a device software image from the 5620 SAM database to a file system

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Images tab button.

3 Perform one of the following:

a To export SR device software images, go to step 4

b To export OmniSwitch software images click on the AOS Software tab button. Go to step 4.

4 Choose an image from the displayed list.

5 Click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported software image and click on the OK button. The software image is saved to files in the specified directory.

7 Close the Software Upgrade form.

Procedure 23-23 To view the deployment, backup/restore, or software upgrade status of an NE

1 Perform one of the following actions.

a Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu to view deployment status. The Deployment form opens with the Incomplete Deployments tab displayed.

i Double-click on a deployment in the list. The deployment properties form opens.

ii View the deployment status.

b Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu to view the backup or restore status. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

i Click on the Backup/Restore Status tab button. The Restore State column of the backup or restore is: Transferring Files, Pending, Reboot, CPM Sync and Reboot, Success, Not Attempted, Save Config, or Failure. The timestamp is also displayed.

ii Double-click on a row in the list to display information about the backup or restore operation. You can click on the General, Backups, Configuration Saves, and Faults tab buttons.

Note — When you click on the Backups tab button, the date and time in the Config File Version column corresponds to the date and time for the Last Boot Cfg Version on the NE.

c Choose Administration→NE Maintenance→Software Upgrade to view the software upgrade status. The Software Upgrade form opens.

i Click on the Software Upgrade Status tab button. A list of NEs displayed.

ii Double-click on an NE in the list to view information about the upgrade. The Software Upgrade Status form opens.

iii Close the Software Upgrade Status form.

2 Close the form.

Procedure 23-24 To view the accounting statistics collection status of an NE

1 Choose Tools→Statistics→Accounting Retrieval Status from the 5620 SAM menu. The Accounting Retrieval Status form opens with a list of managed NEs displayed.

2 Select an NE in the list and click on the Properties button. The Accounting Retrieval Status (View) form opens.

3 View the statistics collection information for the NE.

4 Close the Accounting Retrieval Status (View) form.

5 Close the Accounting Retrieval Status form.

Procedure 23-25 To view the trap metrics information

1 Choose Tools→Statistics→Trap Metrics Information from the 5620 SAM main menu. The Trap Metrics Information form opens and lists the NEs that generated the most traps during the last collection interval. The collection interval is indicated by the Start Collection Period and End Collection Period values at the top of the form.

Note — The number of displayed NEs is limited by the metrics configuration in the nms-server.xml file.

2 Click on the Search button to refresh the trap metrics information. The list and collection interval values are updated.

3 Close the Trap Metrics Information form.

Procedure 23-26 To view an NE file system using an FTP file browser

Perform this procedure to browse and list the files on a managed NE. You require FTP user-account privileges on the NE for access to the NE file system. See chapter 13 for information about enabling FTP access for an NE user account.

1 Initiate an FTP file browser session.

a Use the 5620 SAM main menu.

i Choose Tools→NE Sessions→FTP File Browser. The FTP File Browser form opens.

ii Enter the IP address of the NE that you want to browse in the field at the top of the form.

iii Press Enter or click on the Connect button. The Enter the Username and Password form opens.

Note — When you use the 5620 SAM main menu to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

b Use the Software Upgrade Policy form.

i Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.

ii Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.

iii Click on the More Actions button and choose FTP File Browser. The FTP File Browser form opens.

iv Enter the IP address of the NE that you want to browse in the field at the top of the form.

v Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

iii Click on the More Actions button and choose File Browser. The FTP File Browser form opens, then displays the Enter the Username and Password form.

e Use the topology view of a service.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Topology View button. A Topology View dialog box appears.

v Click on the Yes button. The Service Topology map opens.

vi Right-click on a managed device and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one managed device at a time.

f Use the navigation tree of a service management form.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi On the navigation tree, right-click on a service site and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one service site at a time.

g Use the Sites tab of a service.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi Click on the Sites tab button.

vii Choose a site from the list.

viii Click on the NE Sessions button and choose File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session to only one service site at a time.

h Use the NE alarm contextual menu.

i Select an NE alarm in the 5620 SAM alarm window.

ii Right-click on the alarm and choose NE Sessions→File Browser. The FTP File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

> **Note —** On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.
>
> You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

- **a** Double-click on the directory row in the list.
- **b** Select the directory row and press <CTRL>O.
- **c** Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu, you can browse another NE file system using the same form, if required.

- **i** Click on the Disconnect button to end the browsing session.
- **ii** Go to step 1 a ii.

8 Close the FTP File Browser form.

Procedure 23-27 To view an NE file system using an SSH file browser

Perform this procedure to browse and list the contents of a managed NE using a secure file browser. You require console and SSH user-account privileges on the NE for access to the NE file system, and an SSH server must be configured on the NE. See chapter 13 for information about enabling console or SSH access for an NE user account. See chapter 14 for information about configuring an SSH server for an NE.

1 Initiate an SSH file browser session.

a Use the 5620 SAM main menu.

i Choose Tools→NE Sessions→SSH File Browser. The SSH File Browser form opens.

ii Enter the IP address of the NE that you want to browse in the field at the top of the form.

iii Press Enter or click on the Connect button. The Enter the Username and Password form opens.

b Use the Software Upgrade Policy form.

i Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.

ii Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.

iii Click on the More Actions button and choose SSH File Browser. The SSH File Browser form opens.

iv Enter the IP address of the NE that you want to browse in the field at the top of the form.

v Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The SSH File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

iii Click on the More Actions button and choose File Browser. The SSH File Browser form opens, then displays the Enter the Username and Password form.

e Use the NE alarm contextual menu.

i Select an NE alarm in the 5620 SAM alarm window.

ii Right-click on the alarm and choose NE Sessions→File Browser. The SSH File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP and SSH access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

Note — On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.

You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

a Double-click on the directory row in the list.

b Select the directory row and press <CTRL>O.

c Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu or from the Software Upgrade form, you can browse another NE file system using the same form, if required.

- **i** Click on the Disconnect button to end the browsing session.
- **ii** Go to step 1 a ii.

8 Close the SSH File Browser form.

24 — TCP enhanced authentication

24.1 TCP enhanced authentication overview

This chapter describes the 5620 SAM support of TCP enhanced authentication for NEs based on the MD5 encryption mechanism described in RFC2385. 5620 SAM TCP enhanced authentication allows the use of powerful algorithms for authenticating routing messages.

The 5620 SAM uses a TCP extension to enhance BGP and LDP security. TCP enhanced authentication is used for applications that require secure administrative access at both ends of a TCP connection. TCP peers update authentication keys during the lifetime of a connection.

A 5620 SAM operator with administrative privileges can create, delete, modify, and distribute TCP enhanced authentication components, and can perform an audit of a local key chain to compare it with the associated global key chain or other local key chains. The 5620 SAM TCP enhanced authentication components are called keys and key chains.

Global key chains are created in draft mode. This allows operators to verify that the key chain is correctly configured before they distribute it to the network elements. When the key chain is approved for distribution, you can change the global key chain to released mode, which also distributes the key chain to existing local definitions. The 5620 SAM saves the latest released version of the global key chain.

Caution — Alcatel-Lucent recommends that you use only the 5620 SAM to create keys and key chains. Do not create a key or key chain directly on a managed NE using another interface, for example, a CLI. The 5620 SAM cannot obtain a TCP key secret value from an NE during resynchronization, so it cannot specify the key for use on another NE.

If a local NE key chain and the associated global 5620 SAM key chain differ after a resynchronization, the 5620 SAM raises an alarm.

TCP keys and key chains

A key is a data structure that is used to authenticate TCP segments. One or more keys can be associated with a TCP connection. Each key contains an identifier, a shared secret, an algorithm identifier, and information that specifies when the key is valid for authenticating the inbound and outbound segments.

A key chain is a list of up to 64 keys that is associated with a TCP connection. Each key within a key chain contains an identifier that is unique within the key chain. You can use the 5620 SAM to distribute a global key chain to multiple NEs and assign a key to multiple BGP or LDP instances.

The 5620 SAM treats global and local key chain management as it does policy management; depending on the distribution mode configuration of a local key chain, when you modify a global key chain using the 5620 SAM, all local instances can be updated to ensure that all instances of the key chain in the network are synchronized. See chapter 46 for information about global and local policy instances, policy distribution and distribution modes, and local policy audits.

When the 5620 SAM attempts to synchronize the keys in a global key chain with the keys on an NE, the NE does not return the secret key value. After a key chain is deployed to an NE, the shared secret and the encryption algorithm cannot be modified. You can delete a key chain or key only when it is not in use by a protocol.

You can specify whether an NE uses a TCP key for sending packets, receiving packets, or both. Using keys that are configured for both, or send-receive, is general good practice because communication between NEs cannot be affected by assigning the wrong key type.

There are two classes of TCP keys:

- Active
- Eligible

Active keys

A key set contains one active key. An active key is a key that TCP uses to generate authentication information for outbound segments. You cannot delete the active key in a keychain.

Eligible keys

Each set of keys, called a key chain, contains zero or more eligible keys. An eligible key is a key that TCP uses to authenticate inbound segments.

24.2 Workflow to create a global key chain and local key

1. Create a global key chain that contains at least one key. See Procedure 24-1 for more information.
2. Distribute the key chain to NEs. See Procedure 24-2 for more information.
3. Assign the key chain to a routing protocol, such as BGP or LDP. See chapter 31 for more information.

24.3 TCP enhanced authentication menu

Table 24-1 lists the TCP enhanced authentication menu and the associated functions.

Table 24-1 5620 SAM TCP KeyChains menu

Menu option	Function
Administration→Security→TCP KeyChains	Create and manage TCP keys and key chains.

24.4 TCP enhanced authentication procedures

Use the following procedures to perform TCP enhanced authentication management functions.

Procedure 24-1 To create a global key chain

Perform the following procedure to create a global TCP key chain for distribution to NEs.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Click on the Create button. The KeyChain (Create) form opens.

3 Configure the parameters.

- Displayed Name
- Description
- Send Option
- Receive Option
- Admin State

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click the KeyChain Key tab button.

5 Click the Create button. The KeyChain Key (Create) form opens.

6 Configure the parameters:

- Key ID
- Auto-Assign ID
- Secret Key Algorithm
- Key
- Key Direction
- Admin State
- Begin Time
- End Time
- Tolerance (seconds)

Caution — Alcatel recommends that you choose the Send-receive option for the Key Direction parameter to ensure bidirectional communication between NEs.

Note — The 5620 SAM generates a random default value for the Key parameter. For greater security, Alcatel-Lucent recommends that you accept this value rather than manually enter a value.

7 Click on the OK button. A dialog box appears.

8 Click the OK button. The key is added to the keychain and displayed on the KeyChain (Edit) form.

9 Click the OK button. The KeyChain (Edit) form closes.

10 Close the TCP KeyChains form.

Procedure 24-2 To distribute global key chains to NEs

Perform the following procedure to distribute one or more global TCP key chains to one or more NEs. When you distribute a global key chain, local key chain using the Sync With Global distribution mode allow the NE to receive the key chain.

Note — Local key chains using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global key chain. You must ensure that the distribution mode for the local key chain is set to Sync With Global if you want the NE to receive the distribution of a global key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select one or more key chains in the list.

4 When the key chain is in draft configuration mode, the Distribution option, located under the More Actions button, is disabled and the key chain cannot be distributed to the network elements. You must first release the key chain for distribution by performing the following steps. Releasing the global key chain also distributes the key chain to existing local definitions. Otherwise, go to step 5.

i Click on the Properties button. The Key Chain (Edit) form opens.

ii Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

iii Click on the Yes button. The configuration mode of the key chain is changed to Released.

Warning — When you switch the configuration mode of the global key chain to released, the key chain is distributed to existing local definitions.

iv View the local key chain, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local key chain in the list.

v Close the Key Chain (Edit) form. The TCP KeyChains form reappears.

5 Click the More Actions button and choose Distribute. The Distribute - KeyChain form opens.

6 Select one or more NEs in the Available Nodes list.

7 Click on the right-arrow button. The selected NEs move to the Selected Nodes list.

8 Click on the More Actions button and choose Distribute. The 5620 SAM distributes the key chains to the NEs.

9 Close the Distribute - KeyChain form. The TCP KeyChains form reappears.

10 Configure the distribution mode of the local definitions by performing the following steps.

i Click on the More Actions button and choose Distribution Mode. The Distribution Mode form opens.

ii Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.

v Depending on the distribution mode of the chosen site or sites, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Distribution Mode form. The TCP KeyChains form reappears.

11 Close the TCP KeyChains form.

Procedure 24-3 To verify the distribution of a global key chain to NEs

Perform the following procedure to view a list of the NEs to which the 5620 SAM has successfully distributed a specific TCP key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select a key chain in the list.

4 Click on the Properties button. The KeyChain (Edit) form opens.

5 Click on the Local Definitions tab button. The NEs that have a local instance of the key chain are displayed in a list.

6 View the list of NEs to confirm that the key chain is distributed to the required NEs.

7 Close the KeyChain (Edit) form.

8 Close the TCP KeyChains form.

Procedure 24-4 To modify a key chain or key

Perform the following procedure to modify global or local TCP key chain or key parameters, or to add a key to an existing global or local key chain.

Note — When you modify a key chain or key, the modified object is automatically distributed to the NEs that have a local instance of the key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

a Modify a global key chain.

i Select Global from the Policy scope drop-down menu.

ii Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.

b Modify a local key chain.

i Select Local from the Policy scope drop-down menu.

ii Click on the Select button to choose an NE. The Select a Network Element form opens.

iii Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

iv Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

4 Configure the parameters, if required.

- Description
- Send Option
- Receive Option
- Admin State

5 Click the KeyChain Key tab button. The key chain keys are listed.

6 Modify a key, if required.

i Select a key in the list and click on the Properties button. The KeyChain Key (Edit) form opens.

ii Perform steps 6 to 8 of Procedure 24-1.

7 To add a new key to the key chain, perform steps 4 to 8 of Procedure 24-1.

8 Click the OK button. The KeyChain (Edit) form closes.

9 Close the TCP KeyChains form.

Procedure 24-5 To delete a key chain

Perform the following procedure to permanently remove a local or global TCP key chain.

Caution — Deleting a TCP key chain can be service-affecting. Ensure that you understand the implications of deleting the key chain before you proceed.

Note — You cannot delete a TCP key chain when the Admin State parameter for the key chain is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

a Delete a global key chain.

i Select Global from the Policy scope drop-down menu.

ii Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.

b Delete a local key chain.

i Select Local from the Policy scope drop-down menu.

ii Click on the Select button to choose an NE. The Select a Network Element form opens.

iii Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

iv Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Delete button. A dialog box appears.

4 Click on the OK button. A dialog box appears.

5 Click on the OK button. The 5620 SAM deletes the key chain and removes it from the list.

6 Close the TCP KeyChains form.

Procedure 24-6 To delete a key

Perform the following procedure to permanently remove a key from a local or global TCP key chain.

Caution — Deleting a TCP key can be service-affecting. Ensure that you understand the implications of deleting the key before you proceed.

Note — You cannot delete a TCP key when the Admin State parameter for the key is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

  a Delete a key from a global key chain.

    i Select Global from the Policy scope drop-down menu.

    ii Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.

  b Delete a key from a local key chain.

    i Select Local from the Policy scope drop-down menu.

    ii Click on the Select button to choose an NE. The Select a Network Element form opens.

    iii Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

    iv Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

4 Click the KeyChain Key tab button. The key chain keys are listed.

5 Select a key in the list and click on the Delete button. A dialog box appears.

6 Click on the OK button. The 5620 SAM deletes the key and removes it from the list.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The KeyChain (Edit) form closes.

9 Close the TCP KeyChains form.

Procedure 24-7 To identify differences between a global and local policy or two local key chains

Note 1 — You can cancel the local audit at any time by clicking on the Local Audit Off button on the KeyChain (Edit) form.

Note 2 — The 5620 SAM does not identify differences between the Begin Time and End Time properties of key chains.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Choose a device from the list and click on the OK button. The Select a Network Element form closes and the TCP KeyChains form is updated with the network element IP address.

5 Click on the Search button. A list of local key chains is displayed.

6 Choose the local key chain that you want to compare with another key chain.

7 Click on the Properties button. The KeyChain (Edit) form opens.

8 Click on the Local Audit On button. The Local Audit form opens.

9 From the Policy scope drop-down menu:

- a Choose Global and go to step 10.
- b Choose Local and configure the Local Node IP Address parameter by using the Select button to choose a network element. The Select a Network Element form opens.
  - i Choose a network element and click on the OK button. The Select a Network Element form disappears, and the policy manager form reappears with a list of the local policies for the chosen network element in the bottom panel.
  - ii Go to step 10.

10 Click on the OK button. The Local Audit form closes.

11 View the differences between the key chains by clicking on the tab buttons that are highlighted with an arrow icon to indicate that differences exist on the forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

12 Close the local and global key chain (Edit) forms.

25 — Card migration

25.1 Card migration management overview

You can use a 5620 SAM GUI utility called the Card Migration Event Manager to facilitate the transition to an IOM 3 on one or more 7450 ESS or 7750 SR NEs. The Card Migration Event Manager transfers the existing IOM and MDA configurations to new modules with minimal service interruption.

The 5620 SAM Card Migration Event Manager can do the following:

- Upgrade from an IOM 1 or IOM 2 to an IOM3 while retaining the same MDAs.
- Upgrade from one MDA type to a newer MDA type that has compatible features.
- Upgrade an IOM and the associated MDAs in one operation.

You can perform an immediate migration, or preconfigure one or more migration events for later execution. A migration event can include an NE reboot to put the new hardware configuration into effect immediately after the migration. You can upgrade multiple IOMs and MDAs in one operation to limit the number of required NE reboots to one.

During a migration event, the 5620 SAM identifies the configured objects that are bound to the IOM or MDA, deletes the objects, and then creates the objects on the new IOM or MDA. The old and new configurations are saved in the 5620 SAM database until the migration completes successfully. The 5620 SAM preserves the statistics data and alarm information that is associated with each object.

Restrictions

The following restrictions apply to 5620 SAM card migration event management:

- **General**
  - Only the 5620 SAM admin user, or a user with an assigned administrator scope of command role, can create, modify, or execute a migration event.
  - The migration functions are not available to 5620 SAM OSS clients.
  - You may need to re-enable SNMP on an NE after the NE reboots following a migration event.
  - You can only perform a card migration if the description associated with the cards being migrated do not contain any numerical values.
- **IOM-specific**
  - An IOM downgrade, for example, a migration from an IOM 3 to an IOM 2, is not supported.
- **MDA-specific:**
  - You cannot migrate an empty MDA slot to an MDA.
  - MDA migration is limited to MDAs of the same physical transmission type; for example, migration from a SONET MDA to an Ethernet MDA is not supported.
  - You cannot upgrade an MDA that is integrated with an IOM, for example, an IMM.
  - For MDAs, you can migrate only to an MDA of similar capacity that has the same or a greater number of ports.

The 5620 SAM raises an alarm during a migration event if a target NE is unreachable. After a migration event, the 5620 SAM raises an alarm to indicate migration success or failure.

Table 25-1 lists the supported MDA migration types.

Table 25-1 Supported MDA migration types

Current MDA	MDAs supported by migration
10 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
5 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-Gig Ethernet	4 x 10Gig Extended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance SFP
20 x 100 Ethernet Fx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
20 x 10/100/1000 Ethernet Tx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
2 x 10-Gig Ethernet XFP	2 x 10Gig Extended Performance XFP 4 x 10Gig Extended Performance XFP
20 x 10/100/1000 Ethernet SFP	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-gig Ethernet XFP	4 x 10GigExtended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance XFP
5 x 10/100/1000	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
10 x 10/100/1000 Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
60 x 10/100 Ethernet	48 x 10/100/1000 Ethernet Extended Performance TX

25.2 Workflow to manage card migration

The following is the sequence of high-level actions required to manage card migration.

1 Use the 5620 SAM to back up the device configuration of each target NE.

> **Note —** When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.
>
> A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 23 for information about performing NE backups.

2 Create a card migration event and execute or save it, as required. See Procedure 25-1 for more information.

3 Execute a saved card migration event, as required. See Procedure 25-2 for more information.

25.3 Card migration management procedures

Use the following procedures to perform card migration event management tasks.

Procedure 25-1 To create a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Click on the Create button. The Card Migration Event (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Additional Information
- Auto Reboot

4 Click on the NE Migration Candidates tab button.

5 Click on the Add button. The Select Network Elements - Card Migration Event form opens.

6 Select one or more NEs in the list and click on the OK button. The Select Network Elements - Card Migration Event form closes and the NEs are listed on the Card Migration Event (Create) form.

7 Select one or more NEs in the list and click on the Properties button. The Network Element Migration Candidates form opens.

8 Configure the Auto Reboot parameter.

9 Click on the Ok button. The Network Element Migration Candidates form closes, and a dialog box appears.

10 Click on the OK button.

11 Click on the Card Migration Candidates tab button.

12 Click on the Add button. The Select Cards - Card Migration Event form opens.

13 Select one or more cards in the list and click on the OK button. The Select Cards - Card Migration Event form closes and the cards are listed on the Card Migration Event (Create) form.

14 Select one or more cards in the list and click on the Properties button. The Migration Details (Create) form opens.

15 Configure the New Type parameter in the IOM panel, if required.

16 Configure the New Type parameter in the MDA 1 panel, if required.

17 Configure the New Type parameter in the MDA 2 panel, if required.

18 Click on the OK button. The Migration Details (Create) form closes, and a dialog box appears.

19 Click on the OK button.

20 To execute the migration event immediately, perform the following steps. Otherwise, you can execute the migration later by performing Procedure 25-2.

i Use the 5620 SAM to back up the device configuration of each target NE.

Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 23 for information about performing NE backups.

ii Click on the Apply button. The 5620 SAM saves the card migration event configuration.

iii Click on the General tab to display the Status indicator.

iv Click on the Initiate Migration button. A dialog box appears.

v Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

vi Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

21 Click on the OK button. The Card Migration Event (Create) form closes.

22 Close the Card Migration Event Manager form.

Procedure 25-2 To execute a saved card migration event

1 Use the 5620 SAM to back up the device configuration of each target NE.

> **Note —** When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.
>
> A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 23 for information about performing NE backups.

2 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

3 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

4 Select a card migration event and click on the Properties button. The Card Migration Event (Edit) form opens with the General tab displayed.

5 Click on the Initiate Migration button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

7 Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

8 Click on the OK button. The Card Migration Event (Create) form closes.

9 Close the Card Migration Event Manager form.

Procedure 25-3 To delete a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

3 Select a card migration event and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM deletes the card migration event.

5 Close the Card Migration Event Manager form.

26 — TCA

26.1 TCA overview

You can create policies to raise 5620 SAM alarms based on managed-object statistics. When a statistic counter of an object such as an interface reaches a specified threshold, the 5620 SAM alerts GUI operators using a threshold-crossing alarm, or TCA, based on policy specifications.

A TCA policy includes the following:

- the direction of traffic flow to monitor
- the objects that are associated with the policy
- rules that define properties such as the rising and falling thresholds, and the alarm severity
- custom statistics counters that can be used to monitor statistics based on specified formulas

Note — A TCA is not self-clearing. The 5620 SAM clears a TCA only when the TCA policy contains a falling-threshold rule in addition to a rising-threshold rule, and the alarm severity in the falling-threshold rule is set to cleared.

To enable TCA on an object, you must enable collection of performance statistics on the object. To determine whether a specified statistic exceeds a TCA policy threshold, the 5620 SAM compares the utilization value at each statistics collection to the threshold values in the associated TCA policy.

The 5620 SAM TCA function raises an alarm when a statistic threshold is initially crossed. Rather than raise a new alarm for each successive threshold-crossing event associated with a TCA policy, the 5620 SAM changes the severity of the initial alarm based on the rules defined in the policy.

In the 5620 SAM client GUI, you can associate a TCA policy with a managed object from the TCA policy configuration form, or from the object properties form. You can associate one TCA policy with multiple objects.

Statistics counters

Depending on the monitored object, you can create rules to monitor utilization, packets in error, and packets dropped.

The 5620 SAM allows you to monitor custom TCA statistics. You can create a custom TCA profile and build a formula using statistics counters and constant values. See the *5620 SAM Statistics Management Guide* for more information on statistics counters.

For all statistics counters, you can choose to apply the rule to the delta value, rather than the absolute value. The delta value is the difference between the current value and most recent previous value of the statistic counter.

TCA configuration example

The following example describes the 5620 SAM configuration required to raise a TCA, adjust the alarm severity, and clear the alarm, based on the following utilization specifications:

- Raise a minor alarm if utilization is between 60% and 69%.
- Change the alarm severity to major if utilization rises to between 70% and 79%.
- Change the alarm severity to critical if utilization rises to 80% or higher.
- Change the alarm severity to major if utilization falls below 80%.
- Change the alarm severity to minor if utilization falls below 70%.
- Clear the alarm if utilization falls below 60%.

The following are the TCA rules and associated parameter values required to implement the example alarm behavior:

Rule to raise minor alarm for 60% or higher utilization:

- Alarm Severity—minor
- Threshold (%)—60
- Threshold Direction—Rising Above

Rule to change alarm severity to major for 70% or higher utilization:

- Alarm Severity—major
- Threshold (%)—70
- Threshold Direction—Rising Above

Rule to change alarm severity to critical for 80% or higher utilization:

- Alarm Severity—critical
- Threshold (%)—80
- Threshold Direction—Rising Above

Rule to change alarm severity to major if utilization falls below 80%:

- Alarm Severity—major
- Threshold (%)—80
- Threshold Direction—Falling Below

Rule to change alarm severity to minor if utilization falls below 70%:

- Alarm Severity—minor
- Threshold (%)—70
- Threshold Direction—Falling Below

Rule to clear alarm if utilization falls below 60%:

- Alarm Severity—cleared
- Threshold (%)—60
- Threshold Direction—Falling Below

26.2 Workflow to configure TCA

Perform these steps to configure a TCA policy on a monitored object.

1 Enable performance statistics collection on the object that is to be monitored. For example, Table 26-1 lists the port statistics policy objects required to enable TCA on a network interface or physical link.

Table 26-1 Port statistics policy objects for TCA

Statistics policy type	MIB	MIB entry	Monitored class
NE MIB	IF-MIB	ifEntry	—
Specific MIB	IF-MIB	ifEntry	equipment.PhysicalPort

See the *5620 SAM Statistics Management Guide* for more information about collecting performance statistics.

2 If you are creating custom TCA rules, configure a custom TCA profile. See Procedure 26-1 for more information.

3 Configure a TCA policy. See Procedure 26-2 for more information.

i Configure a TCA policy.

ii Configure utilization, error, and drop TCA rules.

iii If required, configure custom TCA rules using custom TCA profiles.

4 Apply a TCA policy to an object. See Procedure 26-3 for more information.

5 Configure TCA system preferences, as required. See Procedure 26-5 for more information.

26.3 TCA management procedures

The following procedures describe how to manage TCA policies.

Procedure 26-1 To configure a custom TCA profile

Perform this procedure to create a custom TCA profile to apply to a TCA policy.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Choose CustomProfileTCA (TCA Policy) from the object type drop-down menu.

3 Click on the Create button. The CustomProfileTCA (Create) form opens.

4 Configure the parameters:

- Profile ID
- Auto-Assign ID
- Profile Name
- Description

5 Click on the Select button. The Custom Profile TCA (Create) form opens.

6 Configure the filter criteria, if required, and click on the Search button.

7 Select a monitored object from the list and click on the OK button. The Custom Profile TCA (Create) form closes.

8 Configure the Stats Type parameter.

9 Click on the Build Formula button. The Build Formula form opens.

10 Choose a statistic counter from the Counter Field drop-down menu.

11 Click on the Add button.

12 Add as many expressions to the formula as required.

a Add a statistic counter to the formula.

i Click on one of the mathematical operator buttons.

ii Choose a counter from the Counter Field drop-down menu.

iii Click on the Add button.

b Add a constant value to the formula.

i Click on one of the mathematical operator buttons.

ii Enter a number in the Constant Value field.

iii Click on the Add button.

13 Click on the OK button. The Build Formula form closes.

14 Click on the OK button. The CustomProfileTCA (Create) form closes.

15 Close the TCA Policies form.

Procedure 26-2 To configure a TCA policy

Perform this procedure to configure a TCA policy for monitoring object utilization.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Choose TCAPolicy (TCA Policy) from the object type drop-down menu.

3 Click on the Create button. The TCAPolicy (Create) form opens.

4 Configure the parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Description
- TCA Admin State

5 Click on the Select button. The TCAPolicy form opens.

6 Configure the filter criteria, if required, and click on the Search button.

7 Select a monitored object from the list and click on the OK button. The TCAPolicy form closes.

8 Click on the Apply button. The TCAPolicy (Create) form closes and the TCAPolicy (Edit) form opens with the General tab displayed.

Note — The panels that appear on the General tab depend on which object type you are creating a TCA policy for.

9 If applicable, configure utilization TCA rules.

i In the Utilization panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.UtilizationTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.UtilizationTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.

Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

10 If applicable, configure error TCA rules.

i In the Error panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.ErrorTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.ErrorTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.

Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

11 If applicable, configure drop TCA rules.

i In the Drop panel, configure the parameters:

- Disable TCA
- Flow Direction
- Delta Tolerance

ii Click on the Create button in the Rules subpanel. The PercentageTCARule, tca.DropTCA-0 (Create) form opens.

iii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction
- Use for Delta TCA

iv Click on the OK button. The PercentageTCARule, tca.DropTCA-0 (Create) form closes.

v Repeat steps ii to iv to create additional rules, as required.

Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

12 If applicable, configure custom TCA rules.

i In the Custom panel, click on the Create button. The CustomTCA (Create) form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Disable TCA
- Displayed Name
- Delta Tolerance

iii Click on the Select button. The Select Custom Profile TCA - CustomTCA form opens.

iv Configure the filter criteria, if required, and click on the Search button.

v Select a Custom TCA Profile from the list and click on the OK button. The Select Custom TCA Profile - CustomTCA form closes.

vi Click on the Create button in the Rules panel. The CustomTCARule, tca.CustomTCA-0 (Create) form opens.

vii Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold
- Delta Threshold (%)
- Threshold Direction
- Use for Delta TCA

- **viii** Click on the OK button. The CustomTCARule, tca.CustomTCA-0 (Create) form closes.
- **ix** Click on the OK button. The CustomTCA (Create) form closes and a dialog box opens.
- **x** Click on the OK button.

13 Apply the TCA Policy to monitored objects, as required.

- **i** Click on the Monitored Objects tab button.
- **ii** Click on the Add button. The Select form opens.
- **iii** Configure the filter criteria, if required, and click on the Search button.
- **iv** Select one or more objects from the list and click on the OK button. The Select form closes.

14 Click on the OK button. A dialog box opens.

15 Click on the OK button to confirm the changes. The TCAPolicy (Edit) form closes.

16 Close the TCA Policies form.

Procedure 26-3 To apply a TCA policy to objects using the object properties forms

Perform this procedure to apply an existing TCA policy to an object from the object properties form.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Select an object from the Select Object Type drop-down menu.

3 Configure the filter criteria, if required, and click on the Search button.

4 Select an object from the list and click on the Properties button. The properties form for the object opens.

5 If the object is a Physical Link, perform the following steps.

- **i** Click on the End Point A TCA tab button.
- **ii** Click on the Assign button. The Select TCA Policy form opens.
- **iii** Configure the filter criteria, if required, and click on the Search button.
- **iv** Select a TCA policy in the list and click on the OK button. The Select TCA Policy form closes and the TCA policy is listed on the object properties form.
- **v** Click on the End Point B TCA tab button.
- **vi** Click on the Assign button. The Select TCAPolicy form opens.

vii Configure the filter criteria, if required, and click on the Search button.

viii Select a TCA policy in the list and click on the OK button. The Select TCA Policy form closes and the TCA policy is listed on the object properties form.

ix Go to step 10.

6 Click on the TCA tab button.

7 Click on the Assign button. The Select TCAPolicy form opens.

8 Configure the filter criteria, if required, and click on the Search button.

9 Select a TCA policy in the list and click on the OK button. The TCA policy is listed on the object properties form.

10 Close the object properties form.

11 Close the Manage Equipment form.

Procedure 26-4 To delete a TCA policy

Perform this procedure to delete a TCA policy.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The TCA Policies form opens.

2 Configure the filter criteria, if required, and click on the Search button.

3 Select one or more TCA policies in the list and click on the Delete button. The 5620 SAM deletes the TCA policies.

4 Close the TCA Policies form.

Procedure 26-5 To configure the TCA system preferences

1 Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens.

2 Click on the TCA tab button.

3 Configure the parameters:

- Max TCA Alarm Limit
- Max TCA Alarm Reset Synchronization Time
- Max TCA Alarm Reset Interval
- Alarm Severity

4 Click on the OK button. A dialog box opens.

5 Click on the OK button to confirm the action. The System Preferences form closes.

27 — Bulk operations

27.1 Bulk operations overview

The 5620 SAM bulk operations function allows you to create bulk changes to modify a large amount of information. Bulk changes may be deployed to NEs or restricted to the 5620 SAM.

A bulk change can contain thousands of target objects. These objects, referred to as batch items, are grouped into batches for efficient bulk change execution. An operator can execute an entire bulk change or individual batches.

You should regenerate batches each time you execute a bulk change to ensure that each target object that matches the bulk change filter is modified.

If one or more of the batch items fail to change during a bulk change operation, the Batch Status and the Batch Status Summary parameters help identify the items. You can also use the Task Manager to view information about a batch.

27.2 Workflow to manage bulk operations

1. Create a bulk change. See Procedure 27-1 for more information.
2. Generate batches for a bulk change. See Procedure 27-3 for more information.
3. Execute one or more batches in a bulk change. See Procedure 27-3 for more information.
4. As required, stop a bulk change. See Procedure 27-6 for more information.
5. View the bulk change execution results to verify that the bulk change was successful and to identify any items which failed to change. See Procedure 27-5 for more information.

27.3 Bulk operations procedures

Use the following procedures to manage 5620 SAM bulk operations.

Procedure 27-1 To create a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Open the Create Bulk Change form by performing one of the following steps.

a Click on the Create button.

b To create a bulk change by copying values from an existing bulk change, perform the following steps.

i Configure the filter criteria and click on the Search button. A list of bulk operations appears.

ii Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens.

iii Click on the Copy button.

3 Configure the parameters, if required:

- Operation ID
- Auto-Assign ID
- Name
- Description
- Admin State
- Object Type

The Operation ID parameter is configurable when the Auto-Assign ID parameter is disabled.

4 Click on the Next button. The Specify the filter form opens.

5 Configure the filter criteria, as required and perform the following steps. Creating a filter that contains the attributes that you want to change can limit the number of objects generated for the bulk change.

i Click on the Attribute drop down and select an option.

ii Click on the Function drop down and select an option.

iii Click on the Value drop down and select or enter an option.

iv Click on the Add to filter icon. The options are displayed on the filter panel.

v Select AND or OR from the Operators drop down option. Repeat steps i to iv to add more options.

vi Click on Save, the Save Filter form opens.

vii Configure the parameters:

- Filter Name
- Description
- Public

viii Click on the Save button. The Save Filter form closes.

6 Click on the Count button to determine the number of network objects that are affected based on the filter.

7 Click on the View button to list the target objects. The Filtered List form opens.

8 Click on the Search button. A list of target objects is displayed.

9 Click on the Next button. The Specify the attributes form opens.

10 Double-click on the attribute or attribute group in the attribute tree panel that you want to include in the bulk change. The attribute or attribute group appears in the display panel.

11 If you included an attribute or attribute group that you want to exclude from the bulk change, you can remove it by clicking on the Remove icon in the display panel.

12 Perform one of the following on each listed attribute, as required.

a Enter a value in the attribute field. The drop-down menu changes from Unchanged to Set, which means that the attribute changes to the new value when you execute the bulk change.

b Choose Default from the drop-down menu to specify that the attribute is to change to the default value when you execute the bulk change.

c Choose Clear from the drop-down menu. Depending on the object type, the attribute value is cleared or set to the default value when you execute the bulk change.

13 Click on the Next button. The Change review form opens.

14 Configure the parameters, if required:

- Batch Size
- Continue on Failure
- Admin State

15 Click on the Finish button.

16 Click on the Close button. The Create Bulk Change form closes.

17 To create more Bulk Changes, repeat steps 2 to 16.

Procedure 27-2 To modify a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Click on the Summary tab button.

5 Modify the parameters, if required:

- Description
- Batch Size
- Admin State
- Continue on Failure

6 Click on the Spans tab button and specify a span, if required.

7 Click on the OK button. The Bulk Change configuration form closes.

8 Close the Bulk Operations form.

Procedure 27-3 To execute a bulk change

Note 1 — You can only execute one bulk change at a time. All other bulk changes are queued.

Note 2 — You can only generate batches for one bulk change at a time.

Note 3 — You cannot generate batches when a bulk change is executing.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and perform one of the following.

a If the bulk change contains batches, click on the Execute button to execute all of the batches.

> **Note —** Changes made to the network after the batches were generated are not affected by the bulk change batches.

b If the bulk change does not contain batches, or you want to regenerate the batches, perform the following.

i Click on the Properties button. The Bulk Change configuration form opens.

ii If the Generate Batches button is dimmed, perform the following:

- Click on the Summary tab button.
- Set the Admin State parameter to Enable.
- Click on the Batch Summary tab.

iii Click on the Generate Batches button. The batches are generated and listed on the form.

iv To execute only specific batches, choose one or more batches from the list and click on the Execute Selected button.

v To execute all of the batches, click on the Execute All button.

A dialog box appears. You can modify the bulk change confirmation message behavior from the User Preferences form.

4 Click on the Yes button. The 5620 SAM executes the bulk change.

Procedure 27-4 To enable or disable the display of bulk change confirmation messages

Perform this procedure to specify whether the 5620 SAM displays a confirmation message when an operator initiates a bulk change operation.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Enable Confirmation for Bulk Change Actions parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 27-5 To view executed batch information

Note — You can also use the 5620 SAM Task Manager to view information about a batch.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Choose a batch from the list.

5 Click on the Properties button. The Bulk Change Batch configuration form opens with the General tab displayed. View general information about the executed batch.

6 Click on the Batch Items tab button.

7 Click on the Search button. A list of items that were changed in the batch appears with the status of each batch item.

8 To view the parameters for each batch item, choose a batch item from the list and click on the Properties button.

9 Close all of the forms.

Procedure 27-6 To stop one or more bulk changes

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Perform one of the following:

- **a** Choose one or more bulk change to stop from the list.
- **b** Choose one or more batches to stop by performing the following:
  - **i** Choose a bulk change from the list.
  - **ii** Click on the Properties button. A Bulk Change configuration form opens with the Batch Control tab displayed.
  - **iii** Choose one or more batches from the list.

4 Click on the Stop button. A dialog box appears.

5 Click on the Yes button. The bulk change execution stops.

6 Close the forms.

Procedure 27-7 To delete a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change that you want to delete from the list and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The bulk changes is removed from the 5620 SAM.

28 — Object life cycle

28.1 Object life cycle overview

The OLC state specifies whether an object is in maintenance or in-service mode to filter alarms in the Alarms Window. Alarms are generated for objects and services regardless of the OLC State parameter setting. The parameter setting is not sent to the objects or services.

You can set the OLC state for the following objects and services:

- network element
- card slot
- daughter card
- port
- LAG
- composite service
- service
- site
- SAPs (L2 access interfaces and L3 access interfaces)

Caution — Changing the OLC state on an object will also change the OLC state on all of its child objects. The operation could take several minutes to complete, depending on the number of objects affected.

Setting the OLC state

The default value of the OLC state for network elements can be specified in the discovery rules. See chapter 14 for more information about configuring the default OLC state for network elements. The OLC state default value of a child object is inherited from the parent object. The default value of the OLC state for composite services and services can be specified using the nms-server.xml file.

Caution — Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance. Contact your Alcatel-Lucent representative for information about file modification.

When the OLC state of an NE is set to the maintenance mode, all children equipment such as access interfaces, card slots, daughter cards, and ports are set to maintenance mode. The sites on the NE are set to the maintenance mode.

When the OLC state of a composite service or service is set to the maintenance mode, the following related objects are changed:

- sites on which the services reside
- access interfaces (SAPs, L2 and L3 access interfaces)
- SDP Bindings (mesh, mirror and spoke bindings)

When the OLC state of a composite service or services is changed to in service, access interfaces and sites may not change to in service if they belong to equipment objects that are set to maintenance.

See chapter 19 for information about setting the OLC state for network and equipment objects. See chapters 70, 71, 73, 74, 69, 72 and 76 for more information about setting the OLC state for specific services and sites. See the *5620 SAM Parameter Guide* for information about how to configure the OLC State parameter.

The OLC state for a child object is inherited from the parent object. The OLC state of the parent object must be in service to change the OLC State parameter of the child object. You can change the OLC state parameter of the parent object regardless of the OLC state of the child object. However, when a child object has more than one parent object and the OLC state of one parent is set to maintenance, the child object is set to maintenance. The OLC state for a child object cannot be changed if one of the parent OLC states is set to maintenance.

Discovery rules allow the operator to set the default OLC state for the node during discovery. See chapter 14 for information about setting the OLC state during discovery.

You must add the OLC state property to manually created service templates, as described in Procedure 28-5.

28.2 Workflow to set OLC states

1 If required, configure the default OLC state for network elements in the discovery rules. See chapter 14 for more information on configuring discovery rules.

2 As required, configure the OLC state for specific nodes, cards, ports, LAGs, services and alarms, as required.

  i Configure the OLC state from the 5620 SAM main menu. See Procedure 28-3 for more information.

  ii Configure the OLC state from an object configuration form. See Procedure 28-6 for more information.

  iii Configure the OLC state from the Alarm window. See Procedure 28-4 and Procedure 28-1 for more information.

3 If required, configure the OLC state on a service template using the GUI builder. See Procedure 28-5 for more information.

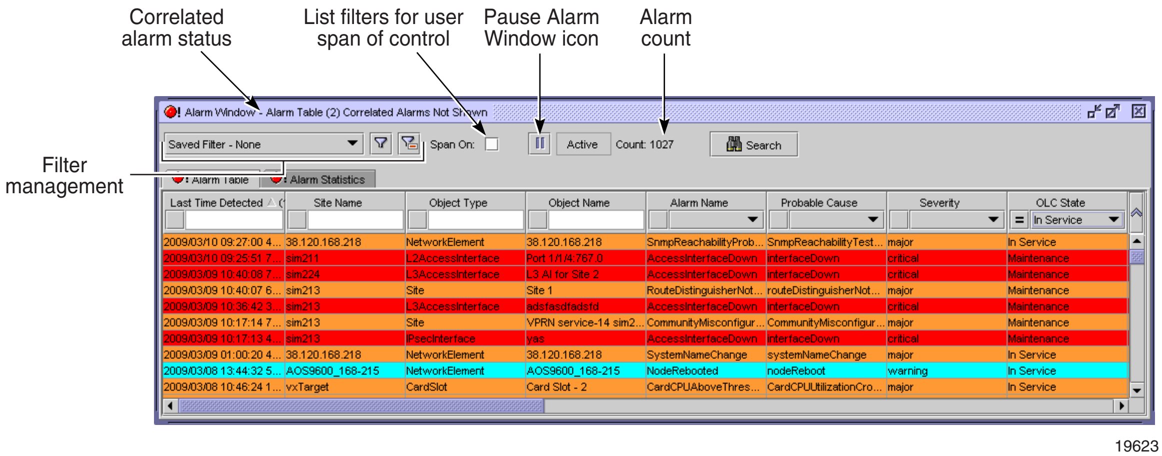
28.3 Setting the OLC state procedures

Use the following procedures to perform OLC management tasks.

Procedure 28-1 To view the OLC state of all network alarms using the dynamic alarm list

The dynamic alarm list Alarm Window allows you to monitor incoming faults from the devices and 5620 SAM software. This feature is most useful when monitoring the network. Figure 28-1 shows the dynamic alarm list Alarm Window.

Figure 28-1 Dynamic alarm list Alarm Window - Alarm Table



1 Click on the filter icon in the Alarm Window. A filter window opens.

Note — You can open and view up to six Alarm Windows. This is useful when you need to view multiple filtered incoming network alarms.

2 Choose OLC State from the Attribute drop-down menu.

3 Configure the filter form to search for alarms. See chapter 3 for more information about creating search filters.

4 To assign the OLC State to the alarm. See Procedure 28-4 for more information.

5 Handle the alarms according to your fault management policies. See the *5620 SAM Troubleshooting Guide* for information about troubleshooting using alarm information guidelines.

Procedure 28-2 To view the OLC state of network equipment or a service

1 Choose Administration→OLC from the 5620 SAM main menu. An OLC form appears.

2 Choose a type of service or object from the object drop-down menu:

- Network Element (network) to view a list of NEs
- Card Slot (physical equipment) to view a list of cards
- Daughter Card Slot (physical equipment) to view a list of daughter cards
- Physical Port (physical equipment) to view a list ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites

3 Choose In Service or Maintenance in the OLC State filter properties using the drop-down menu.

4 Click on the Search button. A list of objects or services appears based on the search filter.

Procedure 28-3 To change the OLC state of equipment or a service

Caution — Changing the OLC state can affect 5620 SAM performance and can take up to ten or more minutes to complete. Changing the OLC state of a parent object changes the OLC state of the child objects.

Note — One JMS message is sent to identify that the OLC state of a parent object has changed.

1 Choose Administration→OLC from the 5620 SAM main menu. An OLC form appears.

2 Choose a type of service or object from the object drop-down menu:

- Network Element (Network) to view a list of NEs
- Card Slot (Physical Equipment) to view a list of cards
- Daughter Card Slot (Physical Equipment) to view a list of daughter cards
- Physical Port (Physical Equipment) to view a list ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites

3 Configure the filter criteria.

4 Click on the Search button. A list of equipment objects or services appears based on the search filter.

5 Select an object in the list. You can select multiple objects.

6 Click on the OLC State button, a drop-down menu appears.

7 Choose Maintenance or In Service from the drop-down menu. The OLC state of the object changes in the filtered list panel.

8 Close the OLC form.

Procedure 28-4 To change the OLC state from the Alarm Window

1. Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.
2. If required, click on the filter icon to create a filtered list of alarms. See chapter 3 for more information about creating search filters.
3. Select an alarm in the list. You can select multiple alarms.
4. Right-click on the alarm, a drop-down menu appears.
5. Choose Assign OLC State. An OLC State Assignment window opens.
6. Choose Maintenance or In service from the drop-down menu.
7. Click on the OK button. A dialog box appears.
8. Click on the Yes button. The OLC State Assignment window closes.

Procedure 28-5 To add the OLC state to a template using the GUI builder

Some service objects have an OLC state property. You cannot configure the OLC state property during the configuration of the service object. For 5620 SAM-created service templates, the OLC state property is automatically added to the template. For manually created service templates, the OLC state property is not added to the template. Perform the following procedure to add the OLC state property to a manually created template.

1. Perform steps 1 to 5 in Procedure 4-6 to open the GUI builder.
2. Perform step 15 in Procedure 4-6 to create a combo box component and enter olcState for the Name combo box component attribute.
3. Enter the value “maintenance” for the List combo box component attribute.
4. Enter the value “inService” for the List combo box component attribute.
5. Enter the value “maintenance” or “inService” for the Default combo box component attribute.
6. Save and close the GUI builder and Script editor windows.

Procedure 28-6 To change the OLC state of an L2 or L3 access interface

Use this procedure to configure the OLC for SAPs on VLL, VPLS, VPRN, MVPLS, and IES services.

Note — The OLC State parameter is configurable on the access interface only when the service OLC State is set to In Service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Perform one of the following actions.

- **a** To choose an L2 access interface
  - **i** Click on the L2 Access Interface tab button.
  - **ii** Choose an L2 access interface and click on the Properties button. The L2 Access Interface (Edit) form opens.
- **b** To choose an L3 access interface
  - **i** Click on the L3 Access Interface tab button.
  - **ii** Choose an L3 access interface and click on the Properties button. The L3 Access Interface (Edit) form opens.

5 Click on the OLC State button, a drop-down menu appears.

6 Choose Maintenance or In Service from the drop-down menu. The OLC state of the object changes in the filtered list panel.

7 Click on the OK button. The service configuration form appears.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button to confirm the action. The service configuration form closes and the Manage Services form reappears.

10 Click on the Close button to close the Manage Services form.

29 — Auto-provision

29.1 Auto-provision overview

Auto-provision provides a way to reuse a proven configuration and apply the configuration to multiple NEs of the same type. This functionality is useful when a large number of similar NEs must be configured. Auto-provision reduces configuration errors and the time to configure each NE. Auto-provision takes advantage of the validations that are executed for every 5620 SAM configuration. When you configure a source NE from a 5620 SAM, the need to troubleshoot configuration problems is reduced.

After a source NE is configured and backed up, an operator can import the source script to the source profile. Alternatively, an operator can add the source script manually to the source profile. From the source profile, a target template can be generated. An operator can import the target template, enter any required changes and deploy the configuration template on a target NE. To ensure that the CLI syntax remains intact, the target NE must be the same type of NE, version, and chassis type as the source NE. For example, a source configuration from a 7705 SAR, version 2.0 device can only be deployed to a 7705 SAR, version 2.0 device.

Auto-provision extends configuration to an adjacent 7750 SR to ensure a prompt and reliable exchange of traffic between the devices. When the configuration profile is successfully deployed to a 7705 SAR target device, the operator can generate configuration modules to configure interactions between the target device and the adjacent devices. An operator can make minor changes to some of the attributes on the configuration modules and deploy the configuration modules to create objects on the selected 7750 SR. When modules are configured, the operator can deploy the modules to configure the connection. A VLL service site is created on the 7705 SAR and the adjacent 7750 SR. The 5620 SAM automatically creates SAPs and SDP bindings.

The 5620 SAM supports the generation of SAP and SDP configuration modules. Configuration between the 7705 SAR and the adjacent 7750 SR requires the following:

- Base configuration of the 7750 SR is complete and the 7705 SAR is auto-provisioned.
- Interface-level configuration is sent to the adjacent 7750 SR.
- The uplink port of the auto-provisioned 7705 SAR is configured to communicate with the network interface of the 7750 SR. Only Ethernet network interfaces are supported.
- The 7750 SR must be able to communicate with the adjacent 7705 SAR.
- A LDP interface is created on the same interface.
- A MPLS interface is created when MPLS is enabled. Choose either RSVP hop by hop or TE.
- MLPPP is configured on the 7750 SR when MLPPP is configured on the adjacent 7705 SAR.
- A LSP is configured between the 7750 SR and the 7705 SAR.
- An Ethernet, TDM or ATM endpoint is created on the 7750 SR that corresponds to the SAP on the 7705 SAR.

The velocity script generator parses a validated source NE configuration so that the NE is compatible with the velocity script management tool that is available in the 5620 SAM. After the layers are identified, the velocity script generator identifies attributes that require configuration before they can be applied to a target NE. Table 29-1 lists the layers that are identified by the velocity script generator. An operator can add, remove, modify, or hide any of the attributes that are listed. The layers must be configured to deploy together.

Table 29-1 Layers and attributes identified by the velocity script generator

Layer	Attributes
Base Equipment layer	SNMP packet size and daughter cards
Channelization layer	SONET SDH paths and channel groups
Policies layer	QoS and ACL related policies
Routing layer	Routing interface configurations and static routes
Routing Protocols layer	Routing Protocol configurations
MPLS layer	Targeted LDP, MPLS interfaces, and LSPs
Service layer	VLL services including Apipe, Cpipe, Epipe, Ipipe, VPRN, SAP, and SDP bindings

Warning — Scripts that are modified and saved must be applied to devices with the same vendor and version.

Access to the script management is controlled by the administration, script management and script execution scope of command roles. Access to auto-provision is controlled by the auto config permissions that are defined in the scope of command roles. Users that are assigned the administration or script management role can create, modify, delete, and execute scripts. Users that are assigned the script execution role can view and run scripts, view and save results, configure script targets and sources, and view historical results.

In addition to the scope of command access roles and profiles, access to the script manager is further defined by span of control. Span of control profiles determine where a user can apply scope of command access roles and profiles. For example, a user may have privileges to execute scripts. However, a span of control profile defines the scripts that the user can execute.

Auto-provision requires a Mobile Services Package license key to operate. See chapter 3 for more information about obtaining and installing software license keys.

29.2 Workflow to configure network devices using auto-provision

1 Configure the source template. See Procedure 29-1 for more information.

- **i** Determine the NE configuration that you need to use for the source.
- **ii** Import a source configuration file from the router, or create a source file by performing a backup of the source configuration and naming the backup file a unique name.
- **iii** Generate a template from the source script.

2 Configure the target template. See Procedure 29-2 for more information.

- **i** Import the template file to the auto-provision profiles manager tool.
- **ii** As required, configure the source script.
- **iii** Use the GUI builder to customize attributes in the source template. Refer to the *5620 SAM Scripts and Templates Developer Guide* for more information.

3 Apply a target template to an unprovisioned NE. See Procedure 29-3 for more information

Note — Typically, step 1 is performed on one 5620 SAM, and steps 2 and 3 are performed on another 5620 SAM. Step 1 is typically performed in a lab or testing environment.

29.3 Auto-provision procedures

Use the following procedures to perform auto-provision.

Procedure 29-1 To configure a source template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profile Manager form opens.

2 Choose Auto-Config Source Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Source Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Select button beside the Source Node Name parameter. The Select Source Node Auto-Config Source Node Profile form opens.

6 Choose a source NE from the list and click on the OK button. The Select Source Node Auto-Config Source Node Profile form closes. The following source NE information is displayed:

- Name
- Management IP Address
- System ID (Loopback IP Address)
- Chassis Type
- Software Version

7 Click on the Apply button. The Backup State parameter displays the status of the last backup operation on the NE, and the Script tab is available.

8 Create a backup file of the source NE and import the configuration script by performing one of the following:

a Back up and import from the router.

i Click on the More Actions button and choose Backup. The Backup State parameter displays the status of the backup. When the status is Success, go to step ii.

ii Click on the More Actions button and choose Attach Source Node Config . The backed-up script is attached to the source profile and can be viewed from the Script tab button.

b Back up and import the device configuration to a file.

i See Procedure 23-4 for information about saving a 7705 SAR configuration to a backup file.

ii Click on the Script tab button and click on the Create button. A Script Editor window opens.

iii Choose File→Import from the Editor menu. The Import dialog box appears.

iv Scroll to the location of the backup file that you previously created and saved.

v Click on the Import button. The script appears in the Script Editor workspace.

vi Choose File→Save and Close from the Editor menu. The Script Editor form closes.

Warning 1 — Scripts that are not correctly applied or created can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define the user responsibilities for script usage, and ensure that scripts are verified before they are executed on devices in a live network.

Warning 2 — Before you run a script, you need read, write, and execute permissions for the following directories:

- *install_dir*/client/nms/bin, in Solaris
- *install_dir*\client\nms\bin\clientCache, in Windows

where *install_directory* is the 5620 SAM client installation location, typically /opt/5620sam/client on Solaris, and C:\5620sam\client on Windows.

vii Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Source Node Profile (Edit) form reappears. The script appears in the list.

9 Click on the More Actions button and choose Generate Template.

Template generation can take several minutes to complete depending on the size of the source configuration file and server resource usage. After the process is complete, the Template tab is available.

10 Click on the Template tab. The newly created template appears in the list.

11 Choose a template and click on the Properties button. The script appears in the Script Editor workspace.

12 See Procedure 4-6 for more information about using the GUI builder tool to generate and customize a UI.

13 Choose File→Save from the Editor menu and close the GUI Builder window. The Script Editor window reappears.

14 Choose File→Export from the Editor menu. The Export dialog box appears.

15 Scroll to the location where you need to save the text file and enter a file name.

16 Click on the Export button. The Script Editor window reappears.

17 Close the Script Editor window. A dialog box appears if you entered any changes to the script.

18 Click on the OK button to save the changes to the script.

19 Close the Auto-Config Source Node Profile (Edit) window.

Procedure 29-2 To configure a target template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profile Manager form opens.

Note — Before you can apply a source configuration to a target NE, you must configure and export the source configuration. See Procedure 29-1 for more information about configuring and exporting a source template.

2 Choose Auto-Config Target Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Target Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Apply button. The Template and Targeted Nodes tabs are available.

6 Click on the Template tab button and click on the Add button. A Script Editor window opens.

7 Choose File→Import from the Editor menu. The Import dialog box appears.

8 Scroll to the location of the file that you exported in Procedure 29-1.

9 Click on the Import button. The script appears in the Script Manager Editor workspace.

10 See Procedure 4-6 for more information about using the GUI builder tool to generate and customize a UI.

11 Choose File→Save from the Editor menu and close the GUI builder window.

12 Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Target Node Profile (Edit) form reappears displaying the template.

13 Close the Auto-Provision Target Node Profile (Edit) window. To apply the source template to a target NE; go to Procedure 29-3.

Procedure 29-3 To apply a target template to an unprovisioned NE

1 Choose Equipment from the drop-down menu on the navigation tree.

Note — You can also access the Auto-Provision Managed Node Wizard from the equipment properties configuration form.

2 Right-click on the target device in the navigation tree and choose Auto-Provision from the drop-down menu. The Auto-Provision Managed Node Wizard form appears with the Profile step displayed.

Note — When a device has been previously configured, the Auto-Provision option is greyed out for the device.

3 Click on the Select button beside the Script ID parameter. A Select Template Name (Profile) - Auto-Provisioning window opens displaying a list of templates.

4 Choose the target template that you configured in Procedure 29-2.

5 Click on the OK button. The Auto-Provision Managed Node Wizard reappears.

6 Perform one of the following:

- **a** Enable the Adjacent NE Managed parameter when the adjacent node is managed by the 5620 SAM. Go to step 9.
- **b** Disable the Adjacent NE Managed parameter when the adjacent node is not managed by the 5620 SAM.

7 Click on the Next button. The Adjacent Node step is displayed.

8 Configure the Adjacent Site ID parameter. Go to step 13.

9 Click on the Next button. The Adjacent 7750 Node step is displayed.

10 Click on the Select button beside the Name parameter. A Select Adjacent NE - Auto-Provision Site window opens with a list of NEs.

11 Choose an NE from the list.

12 Click on the OK button. The Auto-Provision Managed Node Wizard reappears with the information about the displayed NE.

13 Click on the Finish button. A dialog box appears prompting you to deploy the script and generate configuration modules for the adjacent device.

14 Click on the OK button. The 5620 SAM prompts you to view the newly created auto-provision configuration.

15 Enable the View the newly created Auto-Provisioning parameter to display the auto-provision configuration after you close the form, if required.

16 Click on the Close button. The Auto-Provision-Site (Edit) window opens displaying the provisioning for the adjacent device.

17 Click on the Deploy Profile button. A Target Configuration window opens displaying the target NE, and the configurable parameters.

18 Configure the parameters, as required.

19 Click on the NE to which you need to deploy the configuration profile.

20 Click on the Execute button. View the status of the auto-provisioning in the Detailed Status/Error panel. After the NE is configured using the configuration profile, the status of the NE changes to configured.

21 Click on the Modules tab button.

> **Note —** You must deploy the 7750 SR configuration modules after the 7705 SAR auto-provisioning is successfully deployed and resynchronized.

22 Click on the Generate Modules button to prompt the 5620 SAM to display the interactions between the target device and the adjacent device.

23 Click on the Properties button of a generated module to configure all of the modules that were created. The default values for some of the modules are usable. However, for other modules such as SAP modules, the operator must select a port on the 7750 SR before performing step 24.

24 Click on the Deploy Modules button to configure the connection.

25 Click on the Service Associations tab button to view the modified services.

26 Close the Target Configuration window.

Network management

30 — NE routing and forwarding

30.1 NE routing and forwarding overview

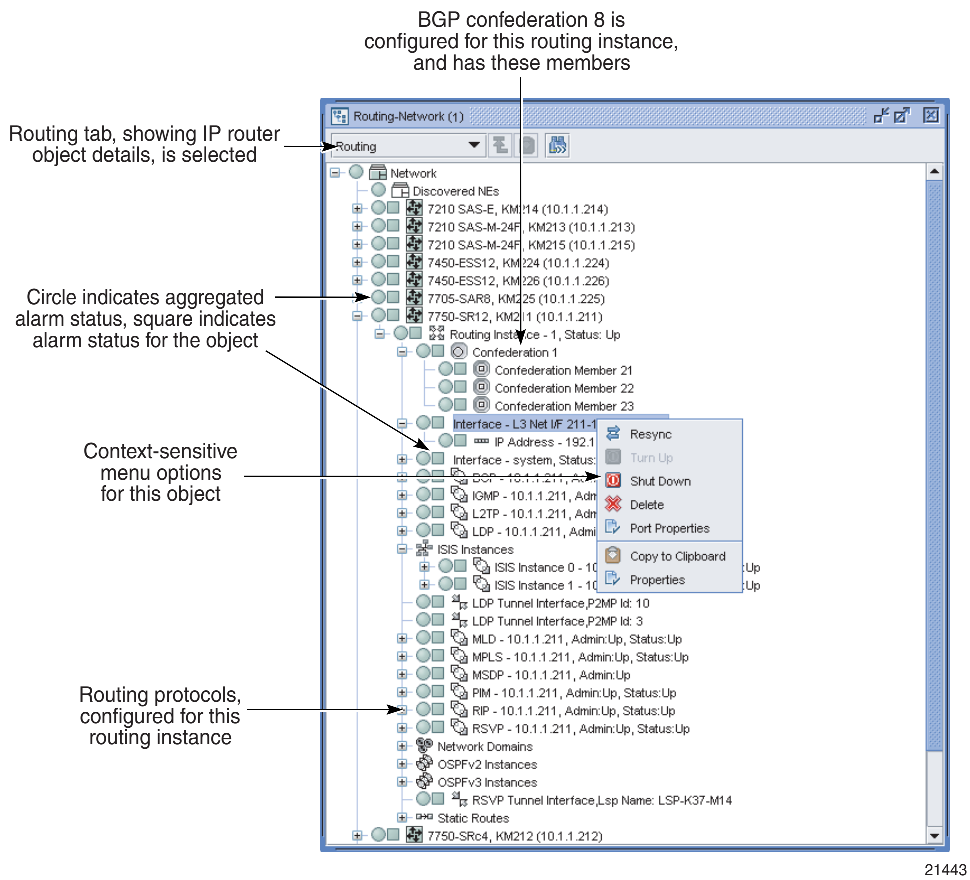
The 5620 SAM allows you to view and configure the routing and forwarding parameters on NEs. You can use the Routing view in the 5620 SAM GUI navigation tree to manage these functions on each managed NE.

Note 1 — For the 7250 SAS-ES and 7250 SAS-ESA, the 5620 SAM supports only the viewing, not the configuration, of routing instances and L3 interfaces. The 7250 SAS-ES and 7250 SAS-ESA must be configured using the CLI before they can be managed by the 5620 SAM.

Note 2 — For an OmniSwitch, the 5620 SAM supports viewing the status of routing protocols that are enabled using the CLI. The 5620 SAM also supports the configuration and management of routing instances, L3 interfaces, and static routes.

Figure 30-1 shows the routing objects in the network view of the navigation tree.

Figure 30-1 Routing objects



L3 network interfaces

An L3 network interface is a logical IP object that is defined on a physical port, such as an Ethernet port. An L3 interface:

- associates an IP address and subnet mask with a physical port or channel
- has a physical port or channel cabled to another device
- requires QoS policy configuration
- requires routing protocol configuration

The physical connection of one device to another device is through a port or channel. However, the L3 interface determines its IP connectivity. The L3 interface passes both routing information and IP traffic.

The system interface is associated with a network entity, such as a specific device, not a specific interface. The system interface is also referred to as the loopback interface. The system interface is associated during the configuration of the following entities:

- the termination point of service tunnels
- the hops when configuring MPLS paths and LSPs
- the addresses on a target device for BGP and LDP peering

The system interface is used to preserve connectivity when an interface fails or is removed. A system interface must have an IP address and a 32-bit subnet mask. The system interface is used as the device identifier by higher-level protocols such as OSPF and BGP. See chapter 31 for more information about routing protocols.

DoS protection

The 7750 SR-7, 7750 SR-12, 7450 ESS-7, and 7450 ESS-12 support the use of DoS protection on network interfaces.

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can use the 5620 SAM to create DoS protection policies and apply them to L3 network interfaces. A DoS protection policy limits the number of control-plane protocol packets that are received each second from a subscriber host, and optionally logs a violation notification if a policy limit is exceeded. The interface drops the excessive packets before they are queued or processed by the NE. You can use the NE System Security form to view the violations for a specific NE.

You can apply DoS protection policies to control the following on L3 network interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each L3 network interface. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

You can also apply DoS protection policies to certain L2 and L3 access interfaces. See the appropriate service chapter for information about applying DoS protection policies to access interfaces.

You can configure global DoS protection on an NE using the NE System Security form. Global DoS protection controls the arrival rate for unprovisioned link-layer protocol packets from CE devices. See Procedure 21-10 for more information.

See Procedure 21-3 for information about configuring NE DoS protection policies. See Procedure 30-9 for information about applying an NE DoS protection policy to an L3 network interface.

Routing protocols

When you configure a device, you configure the routing protocols used and the topology of packet handling between different devices in the network.

Networks can be grouped into areas. An area is a collection of network segments within an AS that have been administratively assigned to the same group. Area topology is concealed from the rest of the AS. This means a significant reduction in routing traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in:

- the same area, known as intra-area routing
- different areas, knows as inter-area routing

In intra-area routing, the packet is routed based on information found within the area; no routing information from outside the area is used. This protects intra-area routing from the injection of bad routing information. Two devices, which are not area border routers, and belonging to the same area, have identical topological databases.

Devices that are aware of more than one area are called area border routers. In this case, all devices in an AS do not have an identical topological database. An area border router has a separate topological database for each area it is connected to. ASs share routing information, such as routes to each destination and information about the route or AS path, with other ASs using BGP.

Routing tables contain lists of next hops, reachable addresses, and associated path cost metrics to each device. Routing protocols use the information and path parameters to compile a network topology. The information about routes that is used to update routing tables can be modified using routing policies.

LLDP

Link Layer Discovery Protocol is a not a routing protocol, but instead, a neighbor-discovery protocol. As such, it is configured in a different manner than the standard routing protocols. LLDP allows a network access device to advertise its identity and capabilities to other stations attached to the same physical IEEE 801 LAN. It also permits information that the devices discover about peer devices to be stored. LLDP is only applicable for devices using Ethernet connectivity.

When LLDP is enabled on a device, it sends and receives LLDP messages on all of the physical interfaces that are enabled for LLDP transmission. These messages are sent periodically to ensure that information is accurate. These messages are stored on the local device for a configurable amount of time, and after this time has expired, the information is discarded.

5620 SAM uses the information stored in the applicable LLDP tables on the node to automatically discover the physical topology in the network. You can use this information to examine the L1/L2 topology and perform appropriate diagnostics and troubleshooting.

In LLDP, a single LLDP Protocol Data Unit is transmitted in a single Ethernet frame. The basic LLDP PDU consists of a header, followed by a variable number of information elements known as TLVs that each include fields for Type, Length, and Value. Type identifies what kind of information is being sent. Length indicates the length of the information string. Value is the actual information sent. Each LLDP PDU includes three mandatory TLVs followed by optional TLVs.

Mandatory TLVs include:

- Chassis ID: this represent the chassis identification of the device transmitting the LLDP frame
- Port ID: this represents the identification of the specific port transmitting the LLDP frame
- TTL: this represents the length of time the receive frame shall be valid

Optional TLVs include:

- Port Description: this represents the description of the port
- System Name: this is the administratively-assigned name of the device
- System Description: this is a textual description of the device
- System Capabilities: this identifies the capabilities of the device and its function (such as router, switch, repeater, etc.)

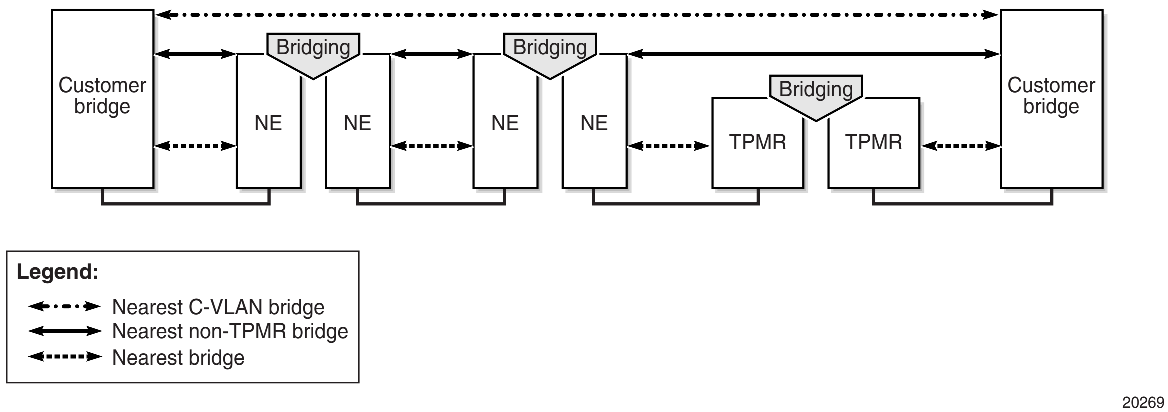
LLDP also supports multiple transmission scopes. The destination MAC address in the LLDP PDU determines how a frame is propagated through the network, thereby determining the LLDP message scope. Table 30-1 identifies a set of destination MAC address and describes the different transmission scopes associated with each address.

Table 30-1 MAC Addresses and transmission scopes

Name	Value	Purpose
Nearest Bridge	01-80-C2-00-00-0E	Propagation constrained to a single physical link
Nearest non-TPMR bridge	01-80-C2-00-00-03	Propagation constrained by all bridges other than TPMR; intended for use within provider bridged networks
Nearest Customer Bridge	01-80-C2-00-00-00	Propagation constrained by customer bridges

This information is also presented graphically in Figure 30-2.

Figure 30-2 LLDP Multiple Transmission Scopes



To enable LLDP, you must configure the protocol at both the system level and at the port level. This is best done using the equipment navigation tree. Table 30-2 lists the procedures required to implement LLDP.

Table 30-2 LLDP configuration procedures list

Procedure	See
To enable LLDP on a router	LLDP in section 30.1 and perform Procedure 17-9
To configure Ethernet ports	Procedure 20-1
To configure OmniSwitch Ethernet ports	Procedure 20-34

You can also use the physical topology map to view and edit various LLDP parameters and interconnections. By default, the physical map displays the topology based on the nearest-bridge LLDP scope. In addition, after the physical topology of a network has been discovered, you can create a reference checkpoint which is basically a snapshot of the topology at a specific time. Any subsequent deviations from this checkpoint can then be displayed. See “Physical topology map” in section 5.1 for more information.

Routing policies

Routing policies, also known as route redistribution policies, control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

The 5620 SAM supports routing-policy distribution to the following devices:

- 7210 SAS-M24F
- 7210 SAS-M24F2XFP
- 7210 SAS-M24F2XFP [ETR]
- 7210 SAS-X24F2XFP
- 7250 SAS and 7250 SAS-ES, at releases earlier than 2.0
- 7450 ESS
- 7705 SAR, Release 1.0 or later
- 7710 SR
- 7750 SR
- Telco, Release 6.0 or earlier

There are no default routing policies. Each policy must be created and applied to an object, a routing protocol, or the forwarding table. Each set of rules that is associated with controlling routes are called routing policy statement entries on the client GUI.

Use routing policies:

- to control routing protocols, such as BGP, to allow routes from another protocol, such as OSPF, into the routing table, which allows the routing table to redistribute packets into other protocols
- to control the import and export of learned active routes of a protocol
- to modify the characteristics of a route, for example, to change the community values of BGP AS path attributes
- to prevent the routes for specific customers from being added to routing tables
- to control BGP route flapping

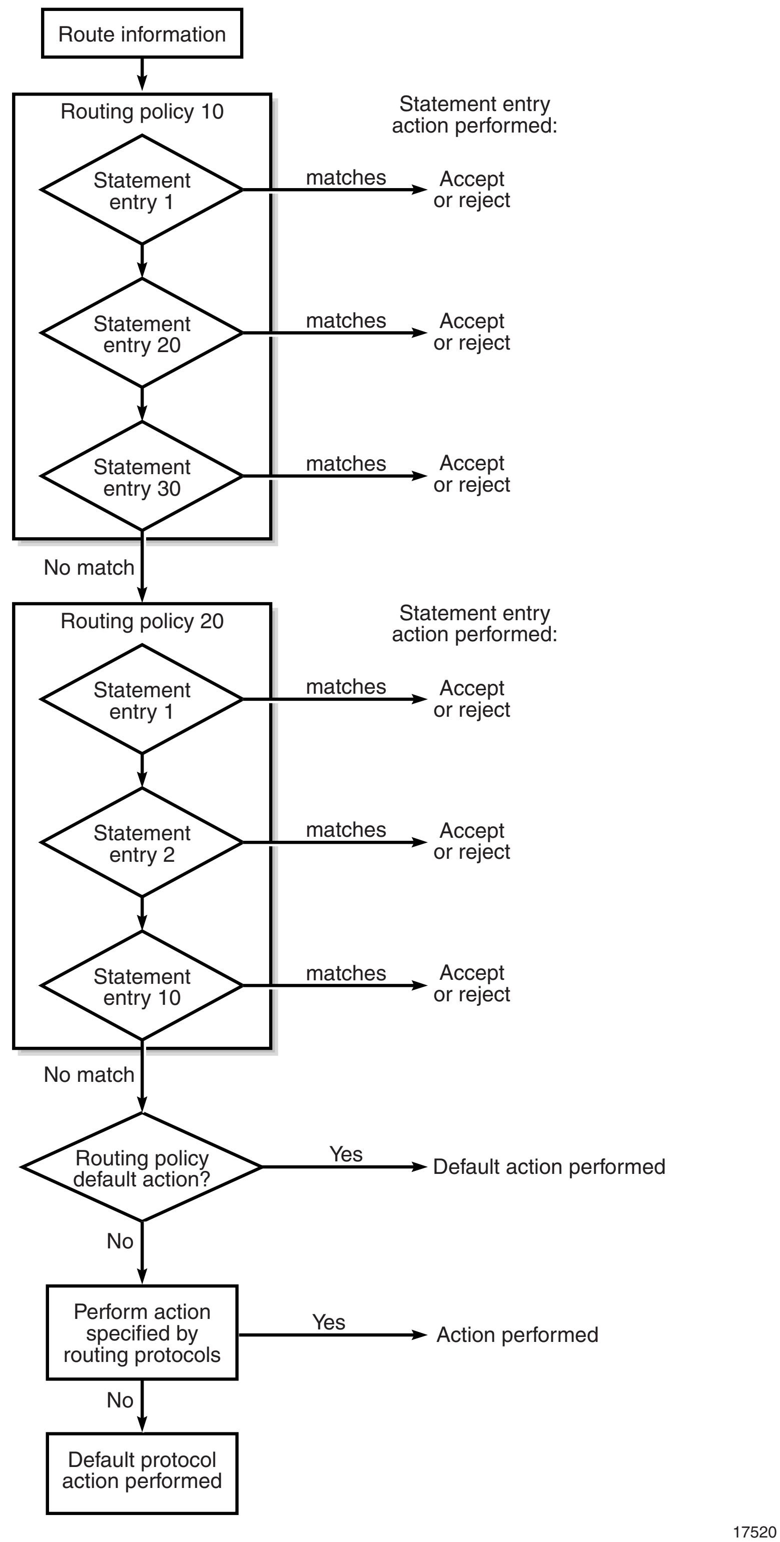
Routing policy statements and routing policy statement entries are compared against incoming route packets in the following sequence.

1. The routing packets arrive.
2. The first routing policy is analyzed.
3. Each entry in the routing policy statement is analyzed.

   If a match is found based on the first routing policy statement entry, the specified action is performed. You can use the Action parameter to specify the continued evaluation of route policy entries, or additional policy statements.
4. If no match is found, the packet is compared against the second routing policy statement entry. If a match is found based on the second routing policy statement entry, the specified action is performed.
5. If no match is found, the packet is compared sequentially against all remaining routing policy statements and routing policy statement entries. If a match is found, the specified action is performed.
6. If the packet does not match any routing policy statements or entries, the default action is performed.

Figure 30-3 shows how routes are analyzed using routing policies.

Figure 30-3 Routing policy analysis workflow



To ensure routing configuration flexibility, the following routing policies can be configured as separate policies or can be cross-referenced to form a framework of policies depending on the network requirements:

- Policy Statement
- Prefix List
- Community
- Damping
- AS Path

Policies that are cross-referenced are distributed together. For example a Policy Statement can reference the Prefix List policy by matching the From Criteria and the To Criteria for each policy type.

Careful planning is essential to implement route policies that can affect the flow of routing information or packets traversing managed devices. Before configuring and applying a route policy, consider the following:

- Develop an overall plan and strategy to accomplish your intended routing actions
- Analyze the effect of what happens to a packet that meets the specified criteria in a routing policy statement entry to ensure the proper action is executed and that no routing loops are created
- when possible, redistribute from a less router protocol to a greater routing protocol, for example from RIP to OSPF
- redistribute exported routes at a single device, when possible

When no action or default action in a routing policy is matched on a packet, then the routing protocols determine the default action for the packet. The action can be specified for the protocol. If the action is not specified, there are default routing protocol import and export actions performed, as described in Table 30-3.

Table 30-3 Default routing protocol actions

Protocol	Default import route action	Default export route options
BGP	All routes from BGP peers are accepted and forwarded to the BGP route selection process.	All active internal BGP routes are advertised to BGP peers. All non-BGP learned routes are not advertised to BGP peers.
IS-IS	IS-IS route acceptance cannot be configured. All IS-IS routes are accepted from IS-IS neighbors.	All internal IS-IS routes are advertised to all IS-IS neighbors. All non-IS-IS learned routes are not advertised to IS-IS neighbors.
OSPF	OSPF route acceptance cannot be configured. All OSPF routes are accepted from OSPF neighbors.	All OSPF routes are advertised to all OSPF neighbors. All non-OSPF learned routes are not advertised to OSPF neighbors.
RIP	All RIP-learned routes are accepted from RIP peers.	All non-RIP learned routes are not advertised to RIP peers.

For importing routing, RIP and BGP learned routes can be altered using routing protocols. For example, for devices learning about routes from BGP, you can create an import route policy that can limit the number and types of routes accepted and added to the routing tables.

For exporting routes, some default behaviors exist:

- internally learned routes are redistributed using the same protocol
- externally learned routes are not automatically advertised to all neighbors or peers

In the case of externally learned routes, you can create an export policy to determine how the routes are advertised, for example, configuring something learned by BGP to be redistributed using OSPF. This is useful in cases:

- where legacy equipment does not support a specific protocol
- when companies merge and they use different routing protocols on the devices

Network Address Translation

Network Address Translation, or NAT, is function that rewrites address information in IP packets that travel between private and public networks. NAT is a widely accepted method of effectively extending the available public IPv4 address space, because multiple end users can share one IP address. NAT can also provide security by preventing an internal IP address, such as an end-user address, from entering a public network.

NAT translates internal, or private, host IP address and TCP port values to external, or public, values. When NAT receives a packet from an internal host, it replaces the source address information in the packet with public address information, and forwards the packet to the destination. NAT assigns private IP addresses and ports dynamically using values from an allocated pool, but can also use values that are statically assigned to internal hosts, depending on the type of NAT depl.oyment.

You can use the 5620 SAM to configure NAT on a Release 8.0 or later 7750 SR-7 or 7750 SR-12, in chassis mode B or higher. 5620 SAM NAT support includes the following:

- policy-based management
- subscriber-specific implementation
- configurable port usage limits per subscriber, address range, or policy
- reserved port ranges for specified forwarding classes that are exempt from port usage limits
- configurable protocol timeout periods for efficient resource management

The 5620 SAM supports the following NAT deployment types:

- L2-aware—Hosts of the same subscriber can share a private address, and are assigned public addresses from a pool in a base routing instance.
- large-scale—Each host can have a unique static or dynamic private address, and is assigned a public address from a pool in a VPRN routing instance.

The NAT configuration on a routing instance includes the following:

- one or more NAT address pools that are associated with local ISA-NAT groups
- a NAT policy, which specifies port ranges and operational parameters
- host address match criteria
- one or more NAT destinations

An ISA-NAT group is a logical group of redundant MDAs that forward NAT packets. A NAT policy associates an address pool with an ISA-NAT group and defines general NAT properties. See chapter 18 for an ISA-NAT group overview and configuration information. See chapter 46 for information about creating and configuring NAT policies.

A 5620 SAM operator assigns port ranges in an address pool configuration. Port ranges specify the number of ports allocated to a subscriber for mapping to host sessions. When all ports for a subscriber are consumed, further port assignments do not occur and host sessions are refused. This helps to prevent the swamping of NAT by an event such as a virus attack or multiple peer-to-peer file transfers. You can override a port-range limit by configuring a range of reserved ports that are assigned based on the traffic forwarding class.

Note — The 5620 SAM does not allow the use of ports 0 to 1023, which are called the well-known ports or privileged ports, in a NAT configuration.

To ensure fair and timely NAT resource allocation to hosts, you can specify timeout values in a NAT policy for protocols such as ICMP, TCP, and UDP. NAT ends a host session after the timeout period, for example, when TCP handshaking takes an unreasonable amount of time.

The NAT drain function is a mechanism that is used to gracefully remove the host sessions associated with an address range in a NAT address pool. When an address range is in the draining state, NAT drops new session requests for the address range. After an existing session associated with a draining address range closes, a new session for the same host is created using a different address range. The drain function removes an address range only when there are no sessions associated with the address range. See chapter 18 for information about using the NAT drain function.

You can view general NAT statistics, for example, address-pool allocation and session counts for different protocols on the Statistics tab of an ISA-NAT group member properties form.

Note — The 5620 SAM does not record detailed NAT session information such as duration or packet counts. You can obtain this information only by directly requesting it from a participating NE.

L2-aware NAT

In L2-aware NAT, a NAT policy is associated with a subscriber profile that is applied to an IES SAP. The NAT policy specifies an address pool on the base routing instance. When DHCP assigns a private IP address that is in an L2-aware NAT address range, NAT assigns a public IP address to the host packets. See chapter 73 for information about configuring NAT in an IES.

Note 1 — A NAT configuration on a base routing instance applies to each IES site on the NE.

Note 2 — A NAT policy that is specified in a subscriber profile redirects all IPv4 traffic for the subscriber to NAT.

Large-scale NAT

Large-scale NAT is used when each host in a customer VPRN service has a unique private IP address and requires a unique public IP address, for example, in mobile network deployments. Large-scale NAT is used between routing instances. A customer VPRN routing instance provides host access and forwards packets through NAT to a VPRN or through an IES to an NE routing instance, which provides public network access.

A VPRN routing instance requires an ACL IP filter or static route to direct host traffic through the NAT function, and uses an address pool in the VPRN routing instance. You can configure large-scale NAT to statically and dynamically assign private addresses. See chapter 74 for information about configuring NAT in a VPRN service. See "Static port forwarding" in this section for more information about configuring NAT to use static private addresses.

Static port forwarding

In a large-scale NAT deployment, you can configure NAT to assign static private addresses to subscriber hosts using static port forwarding. Static port forwarding ensures that an internal host uses the same private IP address and port each time they connect to the network. You can use the 5620 SAM to configure static port forwarding for TCP and UDP independently.

See chapter 74 for information about configuring static port forwarding in a VPRN service. See chapter 68 for information about configuring L2Aware static port forwarding on a residential subscriber instance.

Cflowd

The 5620 SAM supports the configuration of Cflowd on Release 8.0 and later of the 7710 SR, 7750 SR-7 and 7750 SR-12, and on the 7450 ESS in mixed mode. Cflowd is a traffic-sampling function that collects statistical data based on traffic flows. A flow is a series of packets in a user session. Cflowd data is typically used to monitor network-usage trends and detect security threats. You can use the 5620 SAM to configure Cflowd for the following:

- traffic that passes through an L3 network interface
- traffic that is redirected to Cflowd using an ACL IP filter
- AA traffic

You must enable Cflowd globally on an NE before you can configure Cflowd collectors. You can create multiple Cflowd collectors on an NE. Each collector is deleted when Cflowd is disabled.

AA Cflowd is configurable on an ISA-AA group, and supports basic Cflowd sampling as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one Cflowd instance.

See chapter 17 for information about enabling and configuring global Cflowd on an NE, and see chapter 18 for information about enabling and configuring AA Cflowd on an ISA-AA group.

Shared Risk Link Group policies

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. You can use SRLGs to establish a FRR LSP path. You can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path. Links that are members of the same SRLG represent resources which share the same risk. For example, fiber links sharing the same conduit, or multiple wavelengths sharing the same fiber.

An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution, and re synchronization.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. SRLGs indicate to the CSPF which interfaces to avoid in the path's computation.

30.2 Network domain overview

The 5620 SAM allows you to create, delete, associate and edit network domains. You can use the network domains view in the 5620 SAM GUI navigation tree to manage these functions. Network domains help determine which network ports are eligible to transport traffic of individual SDPs. This information is used for the SAP-ingress queue allocation which is applied to VPLS SAPs. No SAP-ingress queues are allocated if a given port does not belong to the network domain used in a VPLS.

Note 1 — A maximum of four network domains are supported in any VPLS.

Note 2 — If an SDP is used for E-PIPE, I-PIPE or A-PIPE bindings, the network domain configuration is not considered.

Note 3 — Network domains are not applicable to loopback and system interfaces.

By default, all network interfaces in a routing instance belong to the default network domain. You can associate an interface to any user defined network domain. The loopback and system interfaces cannot be associated with user defined network domains.

An SDP can be assigned to only one network domain. If no user defined network domain is created, an SDP will be assigned to the default network domain. All SAPs in VPLS will have a queue reaching all fwd complexes serving interfaces belonging to the same network domains as the SDPs. You can assign or remove a network domain association of the interface or SDP without deleting the respective object.

30.3 Workflow to configure NE routing and forwarding

1 Use the CLI to configure or verify the following parameters:

- system address (system ID)
- router ID

See the *7750 SR OS Router Guide* for more information about these parameters.

2 Configure a routing instance.

a If you want to configure a routing instance on the OmniSwitch 6xxx or 9xxx, perform the following:

i Configure a routing instance on the OmniSwitch 6xxx or 9xxx. See Procedure 30-3 for more information.

ii If required, configure UDP relay/DHCP snooping on an OmniSwitch. See Procedure 30-6 for more information.

iii If you configured UDP relay/DHCP snooping, then configure all ports within the network connected to DHCP servers to trusted. See Procedure 20-34 for more information.

b If you want to configure a routing instance on any other NE, see Procedure 30-2 for more information.

3 Create or configure network or system L3 interfaces.

a If you want to configure network or system L3 interfaces on an OmniSwitch, see Procedure 30-8 for more information.

b If you want to configure network or system L3 interfaces on any other NE, see Procedure 30-7 and Procedure 30-9 for more information.

i Associate a network port with the L3 interface.

ii Configure the appropriate routing protocols on the interfaces, as required. The supported protocols are BGP, MPLS, RIP, LDP, OSPFv2, OSPFv3, IS-IS, and RSVP.

See chapter 31 for more information about routing protocol configuration and parameters.

iii Enable the multicast routing types on the interfaces as required. The supported types are PIM, IGMP, and MLD.

See chapter 31 for more information about multicast configuration and parameters.

iv Enable bridging on the interfaces as required. The 5620 SAM supports bridging on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco and OmniSwitch devices.

See chapter 31 for more information about bridging configuration and parameters.

v Assign a DoS protection policy to the interface, if required.

vi Assign an IES or network interface to a virtual router as a VRRP instance.

See chapter 39 for more information about VRRP configuration and parameters.

4 Cable the network ports on the devices to the network ports on other devices.

5 Configure these key device parameters using the 5620 SAM:

- BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP
  Enable routing protocols on the device, as required. If you plan to create signaled LSPs, then you must enable MPLS, and RSVP or LDP.
- IP address ranges for use by services, such as IES and VPLS
  Reserve IP addresses to provide a mechanism to reserve one or more address ranges for services. When services are defined, the address must be in the range specified as a service prefix. Addresses in the range of a service prefix can be allocated to a network port unless set to exclusive. Then, the address range is exclusively reserved for services.
- device-wide AS settings

6 Create static routes, as required. See Procedure 30-20

7 Use the 5620 SAM to configure a routing policy.

i Configure AS path expressions, as required. See Procedure 30-15 for more information.

ii Configure routing policy statements, as required. See Procedure 30-11 for more information.

iii Configure community lists, as required. See Procedure 30-13 for more information.

iv Configure damping parameters to control BGP route flapping, as required. See Procedure 30-14 for more information.

v Configure prefix lists, as required. See Procedure 30-12 for more information.

8 If required, configure an AS and confederations for BGP.

Configuring confederations is optional and should only be implemented to reduce the IBGP mesh inside an AS. An AS can be logically divided into smaller groupings called sub-confederations. See chapter 31 for more information about BGP configuration.

9 Use the 5620 SAM to create MPLS administrative groups and assign the groups to MPLS interfaces and LSPs paths, as required. See Procedure 30-17 for more information.

10 If required, configure NAT on the base routing instance. See Procedure 30-22 for more information.

30.4 Workflow to configure network domains

1 Create a network domain. See Procedure 30-23 for more information.

2 Associate a network interface with a network domain. See Procedure 30-25 for more information.

3 If required, associate a service tunnel with a network domain. See Procedure 30-27 for more information.

30.5 NE routing and forwarding configuration procedures

The following procedures describe how to configure routing.

Procedure 30-1 To query network resources

This procedure describes how to view current network resources such as IP addresses, RDs and RTs, and MAC addresses.

1 Choose Network Resources from the Tools menu. The Network resources form opens with the IP Addresses tab displayed.

2 Select the tab for the particular network resource type you want to query. The choices are:

- IP Addresses
- Route Distinguishers and Route Targets
- MAC Addresses

The form list is refreshed to display the chosen resources.

3 Customize the search as required. Apply a Boolean operator for any of the items in the list header and then do one of the following:

a Choose a specific item type from the adjacent drop down menu (indicated by a downward-pointing arrow).

b Enter a specific string in the adjacent blank text field.

4 Click on the Search button.

The results of your customized search are displayed.

5 Close the Network Resources form.

Procedure 30-2 To configure a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 If you are configuring a VRF routing instance on an OS 9700E or OS 9800E, go to step 4, otherwise go to step 6.

4 Right-click on the OS 9700E or OS 9800E, and choose Create VRF Instance. The Routing Instance (Create) form opens.

5 Configure the VRF Name parameter. Click on the Apply button. The Routing Instance (Edit) form opens. Go to step 8.

6 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

7 Configure the Administrative State parameter.

8 Click on the Protocols tab button.

9 Configure the applicable parameters:

- BGP Enabled
- MPLS Enabled
- OSPFv2 Enabled
- RIP Enabled
- L2TP Enabled
- LDP Enabled
- OSPFv3 Enabled
- IS-IS Enabled

The supported protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 31 for more information about routing protocol configuration using the GUI.

Note — SNMPv3 must be used to manage OS 9700E and OS 9800E NEs, when configuring a VRF routing instance.

10 Click on the More Actions button and choose Edit Routing Policies. A Routing Policy Manager (Edit) window opens.

11 Click on the More Actions button and choose Show Policy. A Routing Policy Show Policy window opens with the General tab displayed.

12 Click on the Ok button. A CLI display is initiated.

13 View the policy.

14 Click on the Close button. The Routing Policy Show Policy window closes.

15 Click on the Multicast tab button.

Multicast is not configurable for the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS.

16 Configure the parameters:

- PIM Enabled
- IGMP Enabled
- MLD Enabled
- MSDP Enabled

The supported multicast protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 31 for more information about multicast protocol configuration using the GUI.

17 Click on the Routing tab button.

18 Configure the parameters:

- Router ID
- Maximum Number of Equal Cost Routes
- Autonomous System
- Confederation Autonomous System
- LDP Shortcut Enabled
- Enforce Maximum Number Of Multicast Routes

Autonomous System, Confederation Autonomous System and Enforce Maximum Number Of Multicast Routes parameters are not configurable in the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS.

When you select the Enforce Maximum Number Of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number Of Multicast Routes
- Log Only
- Threshold (%)

See chapter 31 for more information about AS and confederation parameters for BGP using the GUI.

19 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

20 Configure a Multicast Path Management Info Policy, if required.

i Click on the Select button beside the Name parameter. The Select Ingress Info Policy form is displayed.

ii Choose the required policy from the list and click OK. The Select Ingress Info Policy form closes and the policy name is displayed in the Name field.

Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 46 for a listing of the displayed operational channel parameters.

21 Click on the Interfaces tab button. See Procedure 30-7 for more information about creating additional L3 interfaces.

22 Click on the Address tab button.

23 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button.

The IP Address form opens.

iii Configure the parameters:

- IP Address
- Prefix Length
- Broadcast Address Format

iv Click on the OK button. The IP Address form closes and the Routing Instance form reappears.

Note — The IP Address, Prefix Length, and Broadcast Address Format cannot be changed for the System interface.

24 Click on the Static Routes tab button to view a list of static routes and to add static routes. See Procedure 30-20 for more information.

25 Click on the NAT Configuration tab button to configure NAT on the routing instance. See Procedure 30-22 for more information.

Note — NAT configuration is supported only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher.

26 Click on the RSVP Tunnel Interfaces tab button to create an RSVP tunnel interface entry, if required.

i Click on the Create button. The RSVP Tunnel Interface (Create) form opens.

ii Click on the Select button beside the Lsp Name parameter. The Select - RSVP Tunnel Interface form opens.

iii Select an RSVP tunnel interface and click on the OK button. The Select - RSVP Tunnel Interface form closes and the RSVP Tunnel Interface (Create) form reappears.

iv Configure the Sender Address parameter.

v Click on the OK button. The RSVP Tunnel Interface (Create) form closes.

27 Click on the LDP Tunnel Interfaces tab button to create an LDP tunnel interface entry, if required.

i Click on the Create button. The LDP Tunnel Interface (Create) form opens.

ii Configure the parameters:

- Description
- P2MP ID
- Root Node
- Sender Address

iii Click on the OK button. The LDP Tunnel Interface (Create) form closes.

28 Click on the Multi-Homing Interface tab button to create a multi-homing interface entry, if required. the Multi-Homing Interface (Create) form opens with the General tab displayed.

Note 1 — The Multi-Homing Interface is a loopback interface used in multi-homing resiliency for a pair of protected routers. When it is active, the Primary interface can be used to advertise reachability information of the alternate router to the rest of the network. The Secondary interface is used to resolve routes advertised by the alternate router in the event that router becomes unavailable. This mechanism applies to both IP and VPN traffic.

Note 2 — Only one Primary and one Secondary multi-homing interface may be created for a router.

Note 3 — You can configure a multi-homing interface on the 7750 SR, 7710 SR, and 7450 ESS (in mixed mode) network elements. Chassis mode “D” must be enabled.

i Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Type
- Hold Time (seconds)
- Administrative State

The Hold Time (seconds) parameter only appears if you specify Secondary as the Interface Type.

ii Click on the Addresses tab button. The Multi-Homing Interface Addresses list is displayed.

iii Click on the Create button. The IP Address (Create) form opens.

iv Configure the IP Address parameter.

Note — Only IPv4 addresses are supported when creating the multi-homing interface.

v Click on the OK button. The IP Address (Create) form closes and the new address appears selected in the list.

vi Click on the OK button. The Multi-Homing Interface (Create) form closes.

29 Click on the Route Aggregation tab button to configure route aggregates that can be generated into the virtual router.

i Click on the Create button. The Aggregation (Create) form opens.

ii Configure the parameters, if present:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Aggregator AS
- Aggregator IP Address

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True.

The 7705 SAR-8 supports Summary Only route aggregation only.

30 Click on the BGP Confederations tab button, if present, to view and create BGP confederations. See chapter 31 for more information about BGP confederation configuration.

31 Click on the Service Address Ranges tab button, if present, to provide a mechanism to reserve one or more IP address ranges for use by services, such as IES.

i Click on the Create button. The Service Address Range form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- Exclusive

iii Click on the OK button. The Service Address Range form closes and the Routing Instance form reappears.

32 Configure an override source IP address or L3 interface for use by a selected IP application, if required.

i Click on the Source Address tab button.

ii Click on the Create button. The Source Address form opens.

33 Choose an IP application from the Source IP Application drop-down menu.

34 Perform one of the following:

Note — If you choose the interface index option, the router must already have a network interface or an IES L3 access interface created on the routing instance.

a Choose IP Address in Source Address Termination to specify a source IP address on the node for use by the IP application.

i Enter an IP address in the Source IP Address field.

ii Go to step 35.

b Choose Interface Index in Source Address Termination to use the primary address on the L3 network interface as the source address on the node for the IP application.

i Click on the Select button to choose an interface. The Select Source Address Network Interface form opens. Select an interface in the list and click on the OK button. The IP address and Interface ID of the L3 interface appears on the form.

ii Go to step 35.

Note — You must select an IPv6 Source IP Address to select an IPv6 Source IP Application.

35 Click on the OK button. The Source Address form closes and the Routing Instance form reappears. The IP application source address and parameters appear on the form.

36 Click on the Local DHCP Servers tab button and perform one of the following steps to configure a local DHCP server on the routing instance, if required or applicable.

Note — DHCPv6 server configuration is supported only on a Release 9.0 or later 7450 ESS in mixed mode, or a Release 9.0 or later 7750 SR.

a To configure a local DHCPv4 server on the routing instance go to step 37.

b To configure a local DHCPv6 server on the routing instance go to step 38.

37 Perform the following steps to configure a local DHCPv4 server on the routing instance, if required or applicable.

i Click on the Local DHCP V4 tab button.

ii Click on the Create button. The Local DHCP Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use GI Address

iv Click on the Select button. The Select Local User Database form opens.

v Select a local user database in the list and click on the OK button. The Select Local User Database form closes and the local user database information is displayed on the Local DHCP Servers (Create) form.

vi Configure the following parameters:

- Allow Send Force Renews
- Use Pool From Client

vii Click on the IP Address Pools tab button to assign one or more IP addresses to the local DHCP server.

viii Click on the Create button. The IP Address Pool (Create) form opens with the General tab displayed.

ix Configure the following parameters:

- Pool Name
- Description

x Configure the parameters in the Minimum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xi Configure the parameters in the Maximum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Offer Time panel:

- Minutes
- Seconds

xiii Configure the parameters in the Pool Minimum Free panel:

- Type
- Threshold

xiv Click on the Subnets tab button to add subnets to the DHCP server pool.

xv Click on the Create button. The Subnet (Create) form opens with the General tab displayed.

xvi Configure the parameters:

- IP Address
- Prefix Length
- Free Addresses Minimum Type
- Free Addresses Minimum Threshold
- Maximum Declined Addresses Stored

xvii Click on the Address Ranges tab button.

xviii Click on the Create button. The Subnet Address Range (Create) form opens.

xix Configure the parameters:

- Action
- Start Address
- End Address

Note — You must exclude static IP addresses from the subnet address range because static IP addresses are dedicated.

xx Click on the OK button. The Subnet Address Range (Create) form closes and a dialog box appears.

xxi Click on the OK button. The Subnet (Create) form reappears.

xxii Click on the Options tab button.

xxiii Click on the Create button. The Subnet Option (Create) form opens.

xxiv Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxv Click on the OK button. The Subnet Option (Create) form closes and a dialog box appears.

xxvi Click on the OK button. The Subnet (Create) form reappears.

xxvii Click on the OK button. The Subnet (Create) form closes and a dialog box appears.

xxviii Click on the OK button. The IP Address Pool (Create) form reappears.

xxix Click on the Options tab button.

xxx Click on the Create button. The IP Address Pool Option (Create) form opens.

xxxi Configure the Option parameter.

xxxii If you set the Option parameter to Custom Option, configure the following parameters:

- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxxiii If you set the Option parameter to DNS Name Servers or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

xxxiv If you set the Option parameter to Domain Name, configure the Value parameter.

xxxv If you set the Option parameter to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

xxxvi If you set the Option parameter to Netbios Node Type, configure the Netbios Node Type parameter.

xxxvii Click on the OK button. The IP Address Pool Option (Create) form closes and a dialog box appears.

xxxviii Click on the OK button. The IP Address Pool (Create) form reappears.

xxxix Click on the OK button. The IP Address Pool (Create) form closes and a dialog box appears.

xl Click on the OK button. The Local DHCP Server (Create) form reappears.

xli Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

xlii Click on the OK button. The VPRN Site (Create) form reappears.

38 Perform the following steps to configure a local DHCP v6 server on the routing instance, if required or applicable.

Note — DHCPv6 server configuration is supported only on a Release 9.0 or later 7450 ESS in mixed mode, or a Release 9.0 or later 7750 SR.

i Click on the DHCP V6 tab button.

ii Click on the Create button. The Local DHCPv6 Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use Pool From Client

iv Configure the parameters in the Lease Hold Time panel:

- Days
- Hours
- Minutes
- Seconds

v Click on the IPv6 Address Pools tab button to assign one or more pools to the local DHCPv6 server.

vi Click on the Create button. The IPv6 Address Pool (Create) form opens with the General tab displayed.

vii Configure the following parameters:

- Pool Name
- Description

viii Click on the Prefixes tab button to add prefixes to the DHCPv6 server pool.

ix Click on the Create button. The Prefix (Create) form appears with the General tab displayed.

x Configure the following parameters:

- IPv6 Address
- Prefix Length

xi Configure the parameters in the Preferred Life Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Valid Life Time panel:

- Days
- Hours
- Minutes
- Seconds

xiii Configure the parameters in the Renew Timer panel:

- Days
- Hours
- Minutes
- Seconds

xiv Configure the parameters in the Rebind Timer panel:

- Days
- Hours
- Minutes
- Seconds

xv Click on the Apply button. A dialog box appears.

xvi Click on the OK button.

xvii Click on the Options tab button.

xviii Click on the Create button. The Prefix Option (Create) form appears.

xix Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String, Hex String, or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xx Click on the OK button. The Prefix Option (Create) form closes and a dialog box appears.

xxi Click on the OK button. The Prefix (Create) form reappears with Options tab displayed.

xxii Click on the OK button. The Prefix (Create) form closes and a dialog box appears.

xxiii Click on the OK button. The IPv6 Address Pool (Create) form reappears with Prefix tab displayed.

xxiv Click on the Options tab button.

xxv Click on the Create button. The IPv6 Address Pool Option (Create) form appears.

xxvi Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String, Hex String, or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxvii Click on the OK button. The IPv6 Address Pool Option (Create) form closes and a dialog box appears.

xxviii Click on the OK button. The IPv6 Address Pool (Create) form reappears with Options tab displayed.

xxix Click on the OK button. The IPv6 Address Pool (Create) form closes and a dialog box appears.

xxx Click on the OK button. The DHCP V6 Server (Create) form reappears with IPv6 Address Pool tab displayed.

xxxi Click on the OK button. The DHCP V6 Server (Create) form closes and a dialog box appears.

xxxii Click on the OK button. The Routing Instance (Edit) form reappears.

39 Click on the Self Generated Traffic tab button. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

40 Choose an application to view or edit the DSCP setting.

41 Click on the Properties button. An Application DCSP Marking form opens.

42 Configure the DSCP parameter.

43 Click on the OK button. A dialog box appears.

44 Click on the Yes button.

45 Click on the DSCP Mapping tab button.

46 Select a DSCP mapping in the list and click on the Properties button. The Application DCSP Mapping form opens.

47 Configure the Forwarding Class parameter.

48 Click on the OK button. A dialog box appears.

49 Click on the Yes button.

50 Click on the Dot1p Marking tab button.

51 Select a Dot1p marking entry in the list and click on the Properties button. The Application Dot1p Marking form opens.

52 Configure the Dot1p parameter.

53 Click on the OK button. A dialog box appears.

54 Click on the Yes button. The Routing Instance (Edit) form reappears.

55 Close the Routing Instance (Edit) form.

Procedure 30-3 To configure an OmniSwitch 6xxx or 9xxx routing instance

To configure an OS 9700E or OS 9800E routing instance, see Procedure 30-2.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch 6xxx or OmniSwitch 9xxx→ Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Routing tab button.

5 Configure the Router ID parameter, if required.

6 Click on the Interfaces tab button. See Procedure 30-8 for information about creating additional OmniSwitch L3 interfaces.

7 Click on the Address tab button.

8 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button. The IP Address (Edit) form opens.

iii Configure the parameters, if required:

- IP Address
- Prefix Length

iv Click on the OK button to save the changes. A dialog box appears.

v Select the check box to indicate that you understand the implications of making the change or click on the No button and go to step ix.

vi Click on the Yes button. A dialog box appears.

vii Click on the Yes button. The Routing Instance (Edit) form reappears.

viii Go to step 9.

ix Close the IP Address (Edit) form.

9 Click on the Static Routes tab button to view a list of static routes and to add static routes. See Procedure 30-21 for more information.

10 Click on the OK button to save the configuration. A dialog box appears.

11 Click on the Yes button to verify the action.

12 Close the form.

Procedure 30-4 To view DHCPv6 leases

This procedure describes how to view the DHCPv6 prefixes that the server has given out.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab button.

5 Click on the Local DHCPv6 tab button. The list of associated DHCPv6 servers is displayed.

6 Select a DHCPv6 server from the list and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

7 Click on the More Actions button and choose Show Leases. The Local DHCPv6 Server Show Leases form opens.

8 Perform one of the following:

a To view the entire list of leases that are active on the DHCPv6 server, click OK.

b To view the lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server and click OK.

Note — If the prefix does not exist in the list of leases, a message displays.

c To view the detailed lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server, select the Detail check box, and click OK. The form displays the CLI details for the specific prefix.

9 Close the Local DHCPv6 Server Show Leases form.

10 Close the Local DHCPv6 Server (Edit) form.

11 Close the Routing Instance (Edit) form.

Procedure 30-5 To view DHCPv6 log events

This procedure describes how to view lease not owner and pool unknown log events for local DHCPv6 servers.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Local DHCP Servers tab button.

5 Click on the Local DHCPv6 tab button. The list of associated DHCPv6 servers is displayed.

6 Select a DHCPv6 server from the list and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

7 Click on the Logs tab button. The Lease Not Owner Log and Pool Unknown Log tabs display.

8 Click on the tab button for the type of log that you wish to display. Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

9 Configure the filter criteria and click on the Search button. A list of event logs appears.

10 Select a log entry and click on the Properties button. The Log form opens.

11 View the log entry.

12 Close the Log form.

13 Close the Local DHCPv6 Server (Edit) form.

14 Close the Routing Instance (Edit) form.

Omniswitch DHCP relay and snooping

A DHCP relay agent is a BOOTP relay agent that relays DHCP messages between DHCP clients and DHCP servers on different IP networks. The Omniswitch supports global or per-VLAN BOOTP/DHCP relay service and per-VLAN UDP port relay services.

DHCP Option-82 and DHCP snooping provide security for a DHCP relay service. The DHCP Option-82 switch-level feature allows the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. DHCP Snooping, at the switch or VLAN level, improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table to track access information for each device. DHCP relay Option-82 and snooping cannot be run on the switch at the same time.

DHCP relay and snooping is configured at the default routing instance level, see Procedure 30-6. In addition, per-VLAN DHCP snooping can be enabled on a VLAN site. See procedures 69-1, 69-4, and 69-6 for more information.

It is necessary to configure ports connected to DHCP servers within the network and/or firewall as trusted ports so that necessary DHCP traffic to/from the server is not blocked. Configuring the port mode as trusted also identifies the device connected to that port as a trusted device within the network. See Procedure 20-34 for more information.

Procedure 30-6 To configure UDP relay/DHCP snooping on an OmniSwitch in routing instances

This procedure describes how to configure UDP Relay and DHCP Option-82 and snooping on default routing instances for all OmniSwitch NEs.

Note — For VRF instances on the OS 9700E and OS 9800E NEs, only UDP Relay service is supported.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch → Routing Instance.

Warning 1 — The routing instance must be the default routing instance.

Warning 2 — UDP Server Statistics/UDP Service Statistics will be lost as part of the parent change from Bridge Instance to Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the UDP Relay tab button to configure UDP relay. The UDP Relay General Configuration tab is displayed.

5 Configure the following parameters in the UDP BOOTP/DHCP Relay General Configuration panel.

- Forwarding Delay (seconds)
- Maximum Hops
- Forwarding Option

6 If you need to use the DHCP Option-82 functionality, configure the following parameters in the Relay Information Configuration panel.

- Relay Agent Information Mode
- Relay Agent Information Policy

7 If you need support for PXE devices, configure the PXE Support parameter.

Note — For VRF instances on the OS 9700E and OS 9800E NEs, the following parameters are read only:

- Forwarding Delay (seconds)
- Maximum Hops
- Relay Agent Information Mode
- Relay Agent Information Policy
- PXE Support

The values of these parameters are updated automatically if the corresponding value is modified under the default VRF instance.

8 Click on the DHCP Snooping tab button to configure DHCP snooping.

9 Configure the following parameters:

- DHCP Snooping Mode
- Bypass Option-82 Check
- Option-82 Format Type
- MAC Address Verification
- Option-82 Data Insertion
- Binding Database Mode
- Synchronization Timeout (seconds)
- Action
- Binding Persistency

If you selected the User String option for the Option-82 Format Type parameter, configure the Option-82 User String parameter.

10 Configure UDP port relay services, if required. Click on the Relay Services tab button.

11 Click on the Create button.

12 Configure the UDP Relay Service parameter.

If you selected the Other option, configure the Relay Service Port and Relay Service Description parameters.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button.

15 Click on the Relay Destinations tab button.

16 Click on the Create button. The Create UDP Service Destinations form opens with the Select Relay Service step displayed.

17 Click on the Select button. The Select UDP Service-UDP Relay Service Destination form opens.

18 Choose a UDP relay service from the list. Click on the OK button.

19 If you selected BOOTP/DHCP (67/68) in step 18 and the parameter Forwarding Option is set to Standard, click on the Next button. Otherwise, go to step 22.

20 The Forwarding Address step is displayed.

21 Configure the Forwarding Address parameter, if required.

22 Click on the Next button. The Select VLANs step is displayed.

23 Configure the search filter and click on the Search button. The Select VLANs form displays the VLANs that match the search criteria.

24 Choose one or more VLANs to be used to forward the UDP traffic.

25 Click on the Finish button. The Create UDP Service Destinations form closes and the selected VLANs appear in the relay destinations list.

Procedure 30-7 To create an L3 interface

This procedure describes how to create L3 interfaces. The interfaces you can configure include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Create a new L3 interface by right-clicking on the routing instance icon and choose Create Interface. The Create Network Interface form opens.

Note — The steps that appear on the Create Network Interface form vary, depending on the device type, device version, and the options that are selected during configuration.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- IPv6 Allowed
- MAC Address
- Allow Directed Broadcasts
- Class
- Loopback Enabled
- PIM RP Delayed Up Period
- Cflowd Type
- Trusted
- Admin Link Local Address
- Admin Link Local Address Preferred
- Strip Label
- LDP Synchronization Timer
- FlowSpec Validate Enabled
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6

5 Click on the Next button and perform one of the following:

a If you chose Numbered in the Class parameter in step 4, the Configure IP Address form opens. Specify the IP address information for the L3 interface:

i Click on the Create button. The IP Address (Create) form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- IGP Inhibit
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

iii Click on the OK button to save the changes. A dialog appears.

iv Click on the OK button. The IP Address (Create) form closes and the Configure IP Address form reappears.

b If you chose Unnumbered for the Class parameter in step 4, the Configure Unnumbered Interface form opens. Configure the parameters:

- Unnumbered Type
- Unnumbered Reference

6 Click on the Next button. The Select Port form opens.

Note — If the Loopback Enabled parameter is selected on the Define General Properties form, The Select Port step does not appear in the step menu for the 7450 ESS, 7750 SR, 7705 SAR, and 7710 SR.

7 Associate the L3 interface with a physical port.

i Click on the Select button. The Select Port form opens.

ii Choose a port from the list.

iii Click on the OK button. The port is associated with the L3 interface.

8 Click on the Next button. The Select Network Policy form opens.

9 Click on the Select button in the Network Policy panel to list and choose a network policy for the interface. Network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network.

Note — If you select a network policy with a forwarding class mapped to a queue group queue ID, you must ensure that the mapping queue group queue ID is in the selected Queue Group Template Policy.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

10 Click on the Select button beside the Queue Group Template Policy to list and choose a network egress queue group template policy for the interface. Queue group template policies allow SAP or IP interface forwarding classes to be redirected from the typical queue mapping to a shared queue.

Note 1 — You must ensure that the port you selected in step 7 has a network egress queue group with the same name as the Queue Group Template policy created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

Note 2 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

11 Click on the Next button. The Select ACL Filters form opens.

12 Click on the Select buttons to list and choose Ingress and Egress IPv4 and IPv6 ACL filters for the interface. ACL filters are used to filter out IP traffic that matches user-defined criteria.

13 Click on the Next button. The Configure ICMP form opens.

Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

14 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure ICMPv6 form opens. Otherwise, go to step 15.

Configure the parameters:

- Redirects
- Unreachables
- Packet Too Big
- Param Problem
- Time Exceeded
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Number of Param Problem
- Param Problem Time (seconds)
- Number of Time Exceeded
- Time Exceeded Time (seconds)

15 Click on the Next button. The Configure ARP form opens.

i Configure the Timeout (seconds) parameter.

ii Click on the Create button to statically associate an IP or MAC address to the interface. The Static ARP (Create) form opens.

Configure the parameters:

- IP Address
- Physical Address

iii Click on the OK button. The Static ARP (Create) form closes.

16 Click on the Next button. The Configure Proxy ARP form opens.

Proxy ARP allows a device, such as a router, to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device.

17 Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP

18 Click on the Next button. The Configure Proxy ARP Policies form opens.

19 Configure the parameters:

- Proxy Arp Policy 1
- Proxy Arp Policy 2
- Proxy Arp Policy 3
- Proxy Arp Policy 4
- Proxy Arp Policy 5

20 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure Neighbor Discovery form opens. Otherwise, go to step 26.

21 Click on the Create button to configure a neighbor. The Neighbor Discovery (Create) form opens.

22 Configure the parameters:

- IP Address
- Physical Address

23 Click on the OK button. The Neighbor Discovery (Create) form closes and the Configure Neighbor Discovery form reappears.

24 Click on the Next button. The Configure Proxy Neighbor Discovery form opens.

25 Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 1
- Policy 1
- Policy 1
- Policy 1

Note — You must not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured. The 5620 SAM reorders the policies and moves the policy entered for the Policy 3 parameter to the Policy 2 parameter.

26 Click on the Next button. The Configure NTP form opens.

27 Configure the Broadcast parameter.

Note — When the Broadcast parameter is enabled, a time protocol such as NTP or SNTP must be enabled and configured on the device, or the device ignores broadcast time packets received on the interface. See chapter 13 for information about configuring NTP or SNTP on a device.

28 Click on the Next button. The Configure DHCP - General form opens.

29 Configure IPv4 DHCP for the interface, if required.

i Configure the parameters:

- Enable DHCP Relay
- Description
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Copy To Option 43

Note — The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

ii Click on the Next button. The Configure DHCP - Server form opens.

iii Configure the Server 1 through Server 8 parameters.

30 Click on the Next button. The Configure VRRP form opens.

VRRP instances are members of a virtual router that provides backup if a router fails in a statically configured LAN. VRRP instances are created from network interfaces on a router, either as a master owner through which IP packets are routed before a failover or as a backup non-owner that assumes the packet-forwarding (master) role after a failover. Before you create or add a VRRP instance to a virtual router, ensure that the master and backup interfaces have the same VRID and occupy the same subnet.

31 Perform one of the following:

- **a** If a VRRP instance is not required, click on the Next button until the Unicast RPF form opens in step 40.
- **b** If an IPv4 VRRP instance is required, click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed. See chapter 39 for information about VRRP instances and virtual routers.
- **c** If an IPv6 VRRP instance is required, click on the Next button. The Configure IPv6 VRRP form is displayed. Click on the Create button and the VRRP IPv6 Instance (Create) form opens with the General tab displayed. See chapter 39 for information about VRRP instances and virtual routers.

32 Click on the Next button. The Configure Router Advertisement form opens.

33 Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens with the General tab displayed.

34 Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

35 Click on the Prefix tab button.

36 Click on the Create button. The Router Advertisement Prefix (Create) form opens.

37 Configure the parameters:

- IPv6 Prefix
- Prefix Length
- On-Link Determination
- Autonomous Address Configuration
- Lifetime (seconds)
- No Expiry
- Lifetime (seconds)
- No Expiry

Note — Each Lifetime (seconds) parameter is configurable when the associated No Expiry parameter is disabled.

38 Click on the OK button. A dialog box appears.

39 Click on the OK button. The Router Advertisement Prefix (Create) form closes.

40 Click on the Next button. The Unicast RPF form opens.

41 Configure the parameters:

- URPF Check State
- URPF Check Mode

42 Click on the Next button. The Configure Network Domain form opens.

43 Configure the parameters. You can Add Network Domain or Remove Network Domain.

44 Click on the Next button. The Configure BFD form opens.

45 Configure Bi-directional Forwarding Detection for the interface, if required.

i Set the Administration Status parameter to Up. The configuration form is refreshed with additional parameters.

ii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier

iii To view local and remote session peers, click on the BFD Session tab button. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

iv Click on a session. A properties window opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- "no service", when BFD is disabled
- "in service", when BFD is running
- "out of service", when BFD has failed

v Click on the OK button.

Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 31 for information about enabling and disabling BFD for routing protocols.

46 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure IPv6 BFD form opens and you can configure IPv6 BFD parameters for the interface as in step 51.

47 Click on the Finish button. The Summary form opens.

48 Enable the View the newly created Network Interface parameter to view the interface configuration after closing the form, if required.

49 Click on the Close button. The Create Network Interface form closes.

50 If the View the newly created tunnel parameter in step 48 is enabled, the Network Interface (Edit) form opens with the newly created interface configuration displayed. To configure BFD on the network interface, go to step 51.

51 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button. A configuration form opens.

ii Set the Administration Status parameter to Up. The configuration form is refreshed with additional parameters.

iii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier

iv To view local and remote session peers, click on the BFD Session tab button. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties window opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- "no service", when BFD is disabled
- "in service", when BFD is running
- "out of service", when BFD has failed

vi Click on the OK button.

Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 31 for information about enabling and disabling BFD for routing protocols.

Procedure 30-8 To create an OmniSwitch L3 interface

An L3 interface enables IP routing on a VLAN. Without an L3 interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch →Routing Instance.

3 Right-click on the routing instance icon and choose Create Interface from the contextual menu. The Create Network Interface form opens with the Define General Properties form displayed.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured Primary Status
- Enable Forwarding

5 Click on the Next button. The Configure IP Address form opens.

6 Click on the Create button. The IP Address (Create) form opens.

7 Configure the parameters:

- IP Address
- Prefix Length

8 Click on the OK button. The IP Address (Create) form closes and a dialog box appears.

9 Click on the OK button.

10 Click on the Next button. The Configure Proxy ARP form opens.

11 Configure the Enable Local Proxy ARP parameter.

12 Click on the Next button. The Select VLAN form opens.

13 Click on the Select button. The Select VLAN - Network Interface form opens.

14 Choose a VLAN to which you want to add the interface.

15 Click on the OK button. The Select VLAN - Network Interface form closes.

16 Click on the Finish button. The Summary form opens.

17 Select the View the newly created Network Interface parameter to view the interface configuration after you close the Summary form, if required.

18 Click on the Close button. The Create Network Interface form closes.

Procedure 30-9 To configure an L3 interface

This procedure describes how to configure L3 interface parameters. The interfaces you can modify include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface. The path is Routing→Router→Routing Instance→Interface.

3 Select an interface and choose Properties from the right-click contextual menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab button and configure the parameters, if required. Table 30-4 describes the tabs to choose, as shown when you modify an existing routing interface.

Table 30-4 Description of Network Interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • IPv6 Allowed • MAC Address • Allow Directed Broadcasts • Class • PIM RP Delayed Up Period • Cflowd Type • LDP Synchronization Timer • FlowSpec Validate Enabled • Loopback Enabled • Trusted
Port	To create an association between the L3 interface and a physical port or channel. The system interface is not associated with a port.
Policies	To associate network policies and ingress or egress IP ACL filter policies with the network interface.
Protocols	To view a list of protocols that are enabled on the interface, and to apply protocols. The protocols are: • MPLS • OSPFv2 • OSPFv3 • LDP • IS-IS • RIP
Multicast	To view a list of multicast protocols that are enabled on the interface, and to apply protocols. The protocols are: • PIM • IGMP • MLD
Local DHCP Servers	To assign local DHCP servers. Local DHCP servers are configured on the routing instance and VPRN service. They must be assigned to a network or an L3 interface. To assign local DHCPv6 servers the IPv6 Allowed parameter must be enabled.
Security	To assign a DoS protection policy to a network interface.
RCA Result	To view the results of RCA activities on the network interface
Address	To assign an IP address, subnet and broadcast address format to a network interface. Only one primary IP address can be associated with a network interface.
BFD	To configure BFD parameters

(1 of 2)

Tab	Description
ARP	To configure or view ARP and proxy ARP parameters. Click on the General tab button to configure the minimum time, in seconds, that an ARP entry is stored in the ARP table. Click on the Create button to configure static ARP IP and MAC address parameters. Click on the Proxy ARP tab button to view parameter information.
ICMP	To configure ICMP parameters
ICMPv6	If IPv6 is enabled on the interface, to configure ICMPv6 parameters
Neighbor Discovery	To configure neighbor discovery and proxy neighbor discovery for static routes. Click on the General tab button and Create button to configure neighbor discovery IP and MAC address parameters. Click on the Proxy ND tab button to configure proxy neighbor discovery parameters. [1]
VRRP	To add a VRRP instances to an existing virtual router that assumes routing responsibilities from a failed router in a statically configured LAN
MEPs	To add network interface facility MEPs. Each network interface can support one facility MEP.
Advertisement	To configure router advertisement
DHCP	To configure DHCP Relay parameters
NTP	To enable SNTP broadcasts on the network interface
Statistics	To view L3 network interface statistics
Faults	To view alarms that are raised against the network interface, or related alarms that affect the network interface

(2 of 2)

Note

(1) The Proxy ND tab is available only on the 7750 SR.

5 Click on the Apply button to save the changes.

6 Close the form.

7 Cable the network ports or channels of the device, with L3 interfaces enabled, to other devices configured the same way.

8 Configure routing protocols, as described in chapter 31.

Procedure 30-10 To configure an OmniSwitch L3 interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface by choosing Network→ OmniSwitch →Routing Instance→Interface.

3 Choose an interface and choose Properties from the contextual menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab button and modify the parameters, if required. Table 30-5 describes the tabs.

Table 30-5 Description of OmniSwitch network interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • Configured Primary Status • Enable Forwarding • Encap Type
VLAN	View properties of the VLAN to which the interface is assigned or assign a VLAN to the interface.
Address	Assign an IP address to a network interface or view properties of an assigned address. Only one primary IP address can be associated with a network interface.
ARP	Configure the Enable Local Proxy ARP parameter.
Faults	View alarms that are raised against the network interface, or related alarms that affect the network interface.

5 Click on the Apply button to save the changes.

6 Close the form.

Procedure 30-11 To configure a routing policy statement

See "Routing policies" in section 30.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Statement from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

2 Click on the Create button.

3 Configure the parameters:

- Policy Statement Name
- Description
- Default Action
- Check Dependencies

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

a Click on the Components tab button. Select and right-click on Policy Statement Entry and choose Create Policy Statement Entry. The Policy Statement Entry (Create) form opens with the General tab displayed. Go to step 6.

b Click on the Policy Statement Entries tab button.

5 Click on the Create button. The Policy Statement Entry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Action

7 Perform one of the following:

a If you choose Accept, Next Entry, or Next Policy for the Action parameter, go to step 8.

b If you choose None or Reject for the Action parameter, go to step 14.

8 Click on the Action tab button.

9 Configure the parameters:

- Route Origin
- Route Preference
- BGP Local Preference
- Local Preference Set
- Use Next Hop
- Metric Action
- Interface
- Metric Value
- OSPF, RIP, or ISIS Tag (Hex)
- Next Hop Type
- OSPF Route Type
- Advertise Next Hop Self
- Forwarding Class Name
- Forwarding Class Priority
- Damping Profile Name

10 Click on the Path tab button.

11 Configure the parameters:

- AS Path Name
- BGP AS Path Action
- BGP AS Prepend number
- Prepend Count

12 Click on the BGP Community tab button.

13 Configure the parameters:

- Community Name 1
- Community Action 1
- Community Name 2
- Community Action 2

14 Click on the From Criteria tab button. The Policy Statement Entry (Create) form appears with the General tab displayed.

15 Click on the Select button beside the AS Path Name parameter. A Select Policy Statement Entry - Site form opens.

16 Choose an AS path from the list.

17 Click on the Ok button. The AS Path Name is refreshed with the selected AS Path.

18 Click on the Select button beside the Community List Name parameter. A Select Policy Statement Entry - Site from opens.

19 Choose a community from the list.

20 Click on the OK button. The Community List Name is refreshed with the selected community.

21 Configure the parameters.

- Protocol
- Origin
- State
- Interface Name
- Static Route Tag
- No Route Tag
- Family
- Level
- IS-IS External Route
- OSPF Route Type
- OSPF Area
- OSPF Area Set
- Multicast Source IP Address
- Neighbor IP Address

22 Click on the Select button beside the Multicast Group Prefix List Name parameter. A Select Policy Statement Entry window opens.

23 Choose a policy from the list.

24 Click on the Ok button. The Multicast Group Prefix List Name parameter is refreshed with the selected policy.

25 Click on the Select button beside the IGMP Host Prefix List Name parameter. A Select Policy Statement Entry window opens.

26 Choose a policy from the list.

27 Click on the Ok button. The IGMP Host Prefix List Name parameter is refreshed with the selected policy.

28 Click on the Select button beside the Interface Name parameter. A Select Zone Index From Criteria Site window opens.

29 Choose a site from the list.

30 Click on the Ok button. The Interface Name parameter is refreshed with the selected site.

31 Click on the Select button beside the Neighbor Prefix List Name parameter. A Select Policy Statement Entry window opens.

32 Choose a policy statement from the list.

33 Click on the Ok button. The Neighbor Prefix List Name parameter is refreshed with the selected policy.

34 Click on the Prefix List tab button.

35 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

36 Click on the To Criteria tab button. The Policy Statement Entry (Create) form appears with the General tab displayed.

37 Configure the parameters.

- Protocol
- Instance ID
- All Instances
- Level
- Neighbor IP Address

38 Click on the Select button beside the Neighbor Prefix List Name parameter. A Select Policy Statement Entry window opens.

39 Choose a policy from the list.

40 Click on the Ok button. The Neighbor Prefix List parameter is refreshed with the selected policy.

41 Click on the Select button beside the Interface Name parameter. A Select Zone Index To Criteria Site window opens.

42 Choose an interface from the list.

43 Click on the Ok button. The Interface Name parameter is refreshed with the selected site.

44 Click on the Prefix Lists tab button.

45 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

46 Click on the OK button. A dialog box appears.

47 Click on the OK button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 46-1.

48 Configure the following routing-related policies, if required:

a To configure a prefix list policy, see Procedure 30-12.

b To configure a community policy, see Procedure 30-13.

c To configure a damping policy, see Procedure 30-14.

d To configure an AS path policy, see Procedure 30-15.

e To view a routing policy from a CLI session, see Procedure 30-16.

Procedure 30-12 To configure a prefix list policy

See “Routing policies” in section 30.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy Prefix List Manager window opens.

2 Click on the Create button. The Routing Policy Prefix List (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Prefix List Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Prefix List Members tab button.

5 Click on the Create button. The Prefix List Member (Create) form opens.

6 Configure the parameters:

- Prefix
- Mask
- Type
- Begin Length
- Through Length

The Begin Length and Through Length parameters are configurable when the Type parameter value is set to Range or Through.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Routing Policy Prefix List, Global Policy (Create) window appears with the newly created prefix member.

9 Close the Routing Policy Prefix List, (Create) window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 46-1.

10 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 30-11.

b To configure a community policy, see Procedure 30-13.

c To configure a damping policy, see Procedure 30-14.

d To configure an AS path policy, see Procedure 30-15.

e To view a routing policy from a CLI session, see Procedure 30-16.

Procedure 30-13 To configure a community policy

See “Routing policies” in section 30.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Community from the 5620 SAM main menu. A Manage Routing Policy - Community window opens.

2 Click on the Create button. A Routing Policy - Community, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Community Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Community Members tab button.

5 Click on the Create button. A Community Member Site (Create) window opens.

6 Configure the Community Member parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Routing Policy Community (Create) window is updated with the newly created site.

9 Close the Routing Policy - Community, Global Policy (Create) window.

10 Close the Manage Routing Policy - Community window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 46-1.

11 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 30-11.

b To configure a prefix list policy, see Procedure 30-12.

c To configure a damping policy, see Procedure 30-14.

d To configure an AS path policy, see Procedure 30-15.

e To view a routing policy from a CLI session, see Procedure 30-16.

Procedure 30-14 To configure a damping policy

See “Routing policies” in section 30.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Damping from the 5620 SAM main menu. A Manage Routing Policy - Damping window opens.

2 Click on the Create button. A Routing Policy - Damping, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Damping Name
- Half Life
- Reuse
- Suppress
- Max Suppression

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.

5 Close the Routing Policy - Damping, Global Policy (Create) window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 46-1.

6 Configure the following routing-related policies, if required:

  a To configure a policy statement, see Procedure 30-11.

  b To configure a prefix list policy, see Procedure 30-12.

  c To configure a community policy, see Procedure 30-13.

  d To configure an AS path policy, see Procedure 30-15.

  e To view a routing policy from a CLI session, see Procedure 30-16.

Procedure 30-15 To configure an AS path policy

See "Routing policies" in section 30.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→AS Path from the 5620 SAM main menu. A Manage Routing Policy - AS Path window opens.

2 Click on the Create button. An Routing Policy - AS Path, Global Policy (Create) window opens with the General tab displayed.

3 Configure the parameters:

- Path Name
- Description
- Regular Expression

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 46-1.

5 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 30-11.

b To configure a prefix list policy, see Procedure 30-12.

c To configure a community policy, see Procedure 30-13.

d To configure a damping policy, see Procedure 30-14.

e To view a routing policy from a CLI session, see Procedure 30-16.

Procedure 30-16 To view a routing policy from a CLI session

To view a routing policy from a CLI session, navigate to the previously distributed local routing policy or view navigate to a routing instance by choosing Network→Router→Routing Instance. See Procedure 30-2 for more information.

1 Perform one of the following depending on which routing policy you want to view from a CLI session.

a Choose Policies→Routing→Policy from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

b Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

c Choose Policies→Routing→Community from the 5620 SAM main menu. A Routing Policy Community Manager window opens.

d Choose Policies→Routing→Damping from the 5620 SAM main menu. A Routing Policy Damping Manager window opens.

2 Click on the Search button. A list of policies appears.

3 Choose a policy from the list.

4 Click on the Properties button. A *Policy_type* (Edit) form opens.

5 Click on the Local Definitions tab button. A window appears displaying a list NEs to where the policy was distributed.

6 Choose a site from the list.

7 Click on the Properties button. A *Policy_type* Local Policy (Edit) form opens.

8 Click on the More Actions button and choose Show Policy. A Routing Policy Show Policy window opens with the General tab displayed.

9 Click on the Ok button. A CLI display is initiated.

10 View the policy.

11 Click on the close button.

12 Close the A *Policy_type* Local Policy (Edit) form.

Procedure 30-17 To configure an MPLS administrative group policy

MPLS administrative group policies define administrative groups that can be assigned to MPLS interfaces, LSPs, and LSP paths. After you configure MPLS administrative groups, the administrative groups can be assigned to MPLS interfaces, LSPs, and LSP paths on their respective properties forms. Multiple administrative groups can be assigned to each of these objects.

When establishing LSP and LSP paths, devices are only consider MPLS interfaces which are associated with the same administrative group as the LSP or LSP path. MPLS interfaces advertise administrative group associations using CSPF. This is done using the 32 bit mask which you configure using the Value parameter on the MPLS administrative group policy form.

An administrative group can also be assigned to be explicitly excluded from LSPs and LSP paths. The device cannot use MPLS interfaces in the administrative group to establish LSPs or LSP paths. Administrative group exclusion takes priority over administrative group inclusion.

CSPF must be enabled on LSPs for administrative groups to be relevant. You can enable and configure CSPF on the LSP properties form. When CSPF is enabled on an LSP, it is automatically enabled on associated LSP paths. LSP paths can be configured on the LSP path properties form to inherit additional CSPF, administrative group, and other parameters from LSPs.

This procedure describes how to create MPLS administrative groups. Table 30-6 describes where to find information about assigning MPLS administrative groups to MPLS interfaces, LSPs, and LSP paths.

Table 30-6 MPLS administrative group assignments

To assign groups to	See Procedure
MPLS interfaces	"To create an MPLS interface" in chapter 32
LSPs	"To create a static LSP" in chapter 32
LSP paths	"To configure an LSP path" in chapter 32
	"To configure an LSP on a 7250 SAS device" in chapter 32

1 Choose Policies→MPLS→Administrative Group from the 5620 SAM main menu. The Manage MPLS Administration Groups form opens.

2 Click on the Create button. The Admin Group (MPLS) Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Admin Group (MPLS) Policy (Edit) form is refreshed and the tabs are selectable. Table 30-7 describes the tabs that you can choose to configure the parameters.

Table 30-7 Description of MPLS administrative group form tabs

Tab	Description
Local Definitions	Lists MPLS administrative group policies and allows you to manage administrative group policy distribution.
LSPs	Lists and allows you to manage LSPs to which the administrative group has been assigned.
LSP-Path Bindings	Lists and allows you to manage LSP paths to which the administrative group has been assigned.
Interfaces	Lists and allows you to manage MPLS interfaces to which the administrative group has been assigned.
Faults	List and manage alarms related to the administrative group.

5 Click on the More Actions button and choose Distribute to manually distribute the administrative group policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device.

Procedure 30-18 To configure a Shared Risk Link Group policy

This procedure describes how to create SRLG policies. Table 30-8 describes where to find information about related MPLS and LSP procedures.

Table 30-8 Related MPLS and LSP procedures

To:	See Procedure:
Configure an MPLS instance	"To configure an MPLS instance" in chapter 32
Create an MPLS interface	"To create an MPLS interface" in chapter 32
Configure LSP paths	"To configure an LSP path" in chapter 32

1 Choose Policies→MPLS→Shared Risk Link Group from the 5620 SAM main menu. The Manage Shared Risk Link Group Policies form opens.

2 Click on the Create button.

The Shared Risk Link Group, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Shared Risk Link Group Policy (Edit) form is refreshed and the tabs are selectable. Table 30-9 describes the tabs that you can choose to configure the parameters.

Table 30-9 Description of Shared Risk Link Group Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Shared Risk Link Group policies and allows you to manage policy distribution.
Interfaces	Lists and allows you to manage MPLS interfaces to which the SRLG policy has been assigned.
Faults	List and manage alarms related to the SRLG.

5 Click on the More Actions button and choose Distribute to manually distribute the SRLG policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 46 for more information about policies and policy distribution.

Procedure 30-19 To create a static configuration for a SRLG Policy

This procedure describes how to create a static configuration for a SRLG policy. This differs from the standard SRLG policy described in Procedure 30-18 in that it allows you to manually enter into the SRLG database the SRLG membership for links in the entire network. This is typically done at the 7x50 head-end node and is mutually exclusive with the reading of this information from the traffic engineering database.

There are deployments where the 7x50 head-end node interoperates with routers that do not implement the SRLG membership advertisement using IGP SRLG Type-Length Value (TLV) or sub-TLV. In these situations, you can manually enter the link members of SRLG groups for the entire network at any 7x50 node which needs to signal LSP paths, such as a head-end node.

1 Choose Policies→MPLS→Shared Risk Link Group Static Configuration from the 5620 SAM main menu. The Manage Shared Risk Link Group Static Configuration form opens.

2 Click on the Create button.

The Static Configuration for SRLGs Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Static Configuration for SRLGs Policy (Edit) form is refreshed and the tabs become selectable. Table 30-10 describes the tabs that you can choose to configure parameters or view fault information.

Table 30-10 Description of Static Configuration for SRLG Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Static Configuration for SRLG policies and allows you to manage policy distribution.
Routers	Lists and allows you to manage existing static configuration entries or add new ones.
Faults	List and manage alarms related to the static configuration for SRLGs.

5 Click on the Routers tab button.

6 Click on the Create button. The Router for Static Config for SRLG policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Router ID
- Administrative State

8 Click on the OK button, and then click OK in the confirmation box that appears. The router(s) you added appears in the list on the Routers tab.

9 If you want to add other routers, repeat steps 6 and 7, otherwise, go to step 10.

10 Select one of the routers from the list and click on the Properties button. The Router for Static Config for SRLG policy (Create) window opens with the General tab displayed.

11 Configure the Administrative State parameter.

12 Click on the Interfaces tab.

13 Configure the Interface Ip Address parameter. You can enter this manually or use the Select button to choose from a list.

14 Configure the Displayed Name parameter.

Note — You can associate the same Interface Ip Address parameter with more than one SRLG.

15 Click on the Apply button and repeat steps 10 to 14 to add other entries, or click OK to close the Static Configuration for SRLGs policy (Create) window.

16 If you clicked on Apply in the previous step, you can click on the More Actions button and choose Distribute to manually distribute the Static Configuration for SRLGs policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 46 for more information about policies and policy distribution.

Procedure 30-20 To create a static route

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon. The navigation path is Routing→Router→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the contextual menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Forwarding Class Name
- Forwarding Class Priority
- Destination
- Prefix Length
- Multicast Capable Peers
- Type
- IP Address
- Interface Name
- Unnumbered Interface
- Preference
- Metric
- Administrative State
- Tag
- LDP
- Disallow IGP
- Enable CPE Check
- Target IP Address
- Interval (seconds)
- Drop Count
- Log
- Prefix List Name
- Prefix List Flag

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are only displayed when Enable CPE Check is enabled.

You cannot specify a Prefix List if either BFD Enabled or Enable CPE Check parameters are enabled for the static route.

The Prefix List Flag Prefix List Name parameter is configured.

5 If IPv6 is enabled on the routing instance, click on the Select button beside the Interface Name parameter to choose an IPv6 zone index for the static route. The Select Zone Index - Static Route form opens. Otherwise, go to step 7.

6 Select a zone index in the list and click on the OK button. The Select Zone Index - Static Route form closes and the zone index is displayed in the Static Route (Create) window.

7 Click on the OK button. The Static Route (Create) form closes.

Procedure 30-21 To configure an OmniSwitch static route

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon by choosing Network→OmniSwitch or→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the contextual menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- Destination
- Prefix Length
- Type
- IP Address
- Metric

Note — If the address entered for the IP Address parameter is unreachable by the node, the static route is not created on the node. Use the 5620 SAM to verify that all configured static routes are created successfully on the node by checking the list of static routes for the OmniSwitch routing instance.

5 Click on the OK button to save the configuration. The Static Route (Create) form closes.

Procedure 30-22 To configure NAT on a routing instance

NAT configuration is supported only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the NAT Configuration tab button.

5 Click on the Create button. The NAT Configuration (Create) form opens with the General tab displayed.

6 Click on the Select button to choose a NAT policy. The Select NAT policy form opens.

7 Select a policy in the list and click on the OK button. The Select NAT policy form closes, and the policy name is displayed on the NAT Configuration (Create) form.

8 Click on the Apply button. A dialog box appears.

9 Click on the Yes button.

10 Configure the parameters as required:

- Peer Address
- Steering Route Address Prefix
- Prefix Length
- DS Lite
- Subscriber Prefix Length

11 Perform the following steps to add a DS Lite address.

i Click on the DS Lite Address tab button.

ii Click on the Create button. The Dual Stack Lite Address (Create) form opens.

iii Configure the Address and Tunnel; MTU (bytes) parameters.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Dual Stack Lite Address (Create) from closes and the NAT Configuration (Create) form lists the DS Lite address.

12 Perform the following steps to configure static port forwarding, if required.

i Click on the NAT Static Port Forwarding tab button.

ii Click on the Create button. The NAT Static Port Forwarding Display (Create) form opens.

iii Configure the parameters:

- Type
- Inside IP Address
- Outside IP Address
- Inside Port
- Protocol
- Outside Port
- Lifetime (seconds)
- B4 Address
- AFTR Address

Note — You cannot specify the same set of Inside Port and Protocol values in more than one static port mapping to an Inside IP Address.

You can specify the same Outside Port value in multiple mappings to an Inside IP Address.

iv Click on the OK button. The NAT Static Port Forwarding (Create) form closes, and the NAT Configuration (Create) form lists the new entry.

v Repeat steps ii to iv to assign large scale NAT Static Port Forwards, if required.

13 Perform the following steps to syncronize NAT static port forwards, if required.

i Choose a static port forward from the list and click on the Sync button. The NAT Static Port Forwarding Sync form opens.

ii Click on the Select button in the Targeted Router Instance panel. The Select Targeted Router Instance form opens.

iii Select a router instance from the list and click on the OK button. The Select Targeted Router Instance form closes and the NAT Static Port Forwarding Sync form reappears with the router instance information displayed.

iv Configure the Lifetime (seconds) parameter and click on the OK button. A dialog box appears.

v Click on the OK button.

14 Perform the following steps to configure a NAT pool.

i Click on the NAT Pools tab button.

ii Click on the Create button. The NAT Pool (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Description
- Subscriber Limit
- Exported Address Prefix
- Prefix Length
- Monitored Address Prefix
- Prefix Length
- NAT Pool Type
- Administrative State
- Port Mode
- Port Reservation Type
- Port Reservation Value
- Port Forward Range End
- High Watermark
- Low Watermark

iv Click on the Select button to choose an ISA-NAT group. The Select ISA-NAT group form opens.

v Select an ISA-NAT group in the list and click on the OK button. The Select ISA-NAT group form closes, and the NAT Pool (Create) form displays the ISA-NAT group name.

vi Click on the NAT Pool Ranges tab button.

vii Click on the Create button. The NAT Pool Range (Create) form opens.

viii Configure the parameters:

- Description
- Range Start
- Range End

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The NAT Pool Range (Create) form closes, and the NAT Pool (Create) form lists the pool range.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The NAT Pool (Create) form closes, and the NAT Configuration (Create) form lists the NAT pool.

xiii Repeat steps vii to xii to add another pool, if required.

15 Perform the following steps to add an IP address for L2-aware NAT forwarding, if required.

i Click on the L2 Aware IP Addresses tab button.

ii Click on the Create button. The L2 Aware IP (Create) form opens.

iii Configure the parameters:

- Inside IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L2 Aware IP (Create) form closes, and the NAT Configuration (Create) form lists the IP address.

vi Repeat steps ii to v to add another IP address, if required.

16 Perform the following steps to add a NAT destination address.

i Click on the NAT Destinations tab button.

ii Click on the Create button. The NAT Destination (Create) form opens.

iii Configure the parameters:

- Inside IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The NAT Destination (Create) form closes, and the NAT Configuration (Create) form lists the destination.

vi Repeat steps ii to v to add another destination, if required.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The NAT Configuration (Create) form closes, and the NAT configuration is listed on the Routing Instance form.

30.6 Network domain configuration procedures

Perform these procedures to configure a network domain.

Procedure 30-23 To create a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Create Network Domain from the contextual menu. The Network Domain (Create) form opens.

4 Enter:

- Domain Name
- Description

5 Click on the OK button. The Domain Network (Create) form closes and a network domain is created in the navigation tree.

Procedure 30-24 To delete a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Delete from the contextual menu. A Confirm dialog box opens.

Caution 1 — The default network domain cannot be deleted.

Caution 2 — The network domain related to the Interface and SDP cannot be deleted.

4 Perform one of the following:

a Click on the No button to avoid deleting the network domain. The Confirm dialog box closes.

b Click on the Yes button. The network domain is deleted from the navigation tree.

Procedure 30-25 To associate a network interface with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and click on Add Network Interface. The Add Network Interface window opens.

4 Click on Search to display all the Network Interfaces. Select a Network Interface and click on OK the selected Network Interface is displayed on the Network Domain window.

Procedure 30-26 To remove a network interface from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and select the Network Interface that has to be removed from the domain.

4 Click on Remove Network Interface.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the network interface. The Confirm dialog box closes.

b Click on the Yes button. The network interface is removed from the network domain.

Procedure 30-27 To associate a service tunnel with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and click on Add Tunnel. The Add Tunnel window opens.

4 Click on Search to display all the service tunnels. Select a service tunnel and click on OK the selected service tunnel is displayed on the Network Domain window.

Procedure 30-28 To remove a service tunnel from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and select the service tunnel that has to be removed from the domain.

4 Click on Remove Tunnel.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the service tunnel. The Confirm dialog box closes.

b Click on the Yes button. The service tunnel is removed from the network domain.

Procedure 30-29 To edit a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance

3 Choose the newly created interface and right-click on the Interface and select Properties. The Network Interface form opens. See Procedure 30-7, steps 42 and 43 to associate a network interface to a network domain.

4 Select the Network Domain tab. The Network Domain form opens. See Procedure 30-7, steps 42 and 43 to edit a network domain.

---

31 — Protocol configuration

31.1 Protocol configuration overview

The 5620 SAM allows you to configure routing protocols and navigate to the device parameters. One device can support multiple routing protocols.

You use the network, IS-IS, and OSPF views in the 5620 SAM GUI navigation tree to view and configure parameters that set and manage the device routing protocol support. The routing protocols are enabled on the devices when you configure the devices. You configure the Layer 3 interfaces when you configure the routing instance on the device. You can then configure the routing protocols for specific Layer 3 interfaces.

Supported routing protocols include:

- BGP
- RIP
- LDP
- IS-IS
- OSPF
- RSVP
- L2TP

Routing protocols can be configured to import or export routes from other routing protocols using routing policies. See "Routing policies" in section 30.1 for more information.

In addition to routing protocols, the 5620 SAM supports the following router configurations:

- multicast protocols
    - PIM; see section 31.22 for more information
    - IGMP; see section 31.23 for more information
    - MSDP; see section 31.24 for more information
    - MLD; see section 31.25 for more information
- bridging on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices; see section 31.26 for more information

Note — You cannot use the 5620 SAM to configure routing protocols on the 7250 SAS.

IPv6 support

The 5620 SAM supports IPv6 for control-plane addressing on the 7750 SR in chassis mode B (in mixed mode, for 7750 SR-7 and 7750 SR-12 only), C and D, on the 7710 SR, and on the 7450 ESS in mixed mode. See chapter 19 for information about chassis modes.

Although the implementation of IPv6 is driven by the diminishing IPv4 address space, it is increasingly necessary to use a protocol that is designed to handle more complex network applications, such as broadband voice and video transmission, IP transit, Internet exchange peering, and other large enterprise applications.

Transition from IPv4 to IPv6

The transition from IPv4 to IPv6 is occurring in stages as network providers, service providers, and end users migrate existing applications and equipment to the new version. Control-plane forwarding of IPv6 packets is an important part of this transition; it allows isolated IPv6 hosts and smaller IPv6 networks to peer across an IPv4 network, using a mechanism such as 6over4 tunneling.

With 6over4 tunneling, a host encapsulates IPv6 packets in IPv4 packets for transport across an IPv4 network. Routers that identify 6over4 encapsulation remove the IPv4 encapsulation before they forward the packets to other native IPv6 hosts. The 6over4 mechanism uses the IPv4 multicast infrastructure for neighbor discovery.

IPv6 benefits

The general benefits of IPv6 include:

- **simplified header format and fixed header length**

  An IPv6 header contains fewer fields than an IPv4 header. IPv6 excludes obsolete IPv4 header fields and processes option fields only when they contain values. IPv6 also standardizes the size of the packet header to 40 bytes to streamline packet processing. These features reduce packet-processing overhead and make routing more efficient.
- **addressing enhancements**

  IPv6 increases the IP address size from 32 bits to 128 bits to support a greater number of nodes and to provide a more versatile addressing hierarchy. IPv6 also supports address autoconfiguration.

  The scalability of multicast routing is improved by the presence of a Scope field. IPv6 introduces anycast addressing, which designates a group of disparate nodes as the recipient of a specific data stream.
- **improved scalability and extensibility**

  Built-in traffic optimization makes IPv6 highly scalable, and IPv6 supports future routing technology enhancements using protocol extensions.
- **flow-labeling capability**

  IPv6 features packet prioritization which allows the labeling of packets that require special handling, such as real-time service for VoIP conferences.
- **improved privacy and security**

  Authentication, encryption, and data integrity features are mandatory components for which IPv6 supports standardized extensions.

The 5620 SAM and IPv6

The 5620 SAM entities that support IPv6 configuration include the following:

- BGP for base routing instances and VPRN services
- IS-IS adjacencies
- multicast routing
- static routes
- ICMP
- routing policies
- access ingress and egress policies
- CPM filter policies
- PPP
- IES and VPRN SAPs
- IES and VPRN bi-directional forwarding detection
- VLL Ipipe
- PIM-SSM

A 5620 SAM operator enables IPv6 on an interface during interface creation.

The benefits of the 5620 SAM IPv6 implementation include:

- integration with existing IPv4 configurations on many property and configuration forms
- automatic validation of IP addresses on the client GUI, regardless of the IP version
- support of compressed IPv6 addresses when repeated address octets are present
- support for IPv6 statistics
- simultaneous IPv4 and IPv6 support by routing protocols
- separate IPv4 and IPv6 administrative and operational states on an interface

Accepted IPv6 address formats

The 5620 SAM accepts IPv6 addresses in the following formats:

- colon-hexadecimal, or *x:x:x:x:x:x:x:x*
  where *x* is a 16-bit hexadecimal number from 0 to FFFF
- a combination of colon-hexadecimal and dotted-decimal, or *x:x:x:x:x:x:d.d.d.d*
  where
  x is a 16-bit hexadecimal number from 0 to FFFF
  d is an 8-bit decimal number from 0 to 255

Using a combination of colon-hexadecimal and dotted-decimal formats may be convenient in an environment that supports the use of IPv4 and IPv6 addresses.

The 5620 SAM allows IPv6 address compression for an address that contains repeated zero values. You can use two adjacent colons to represent any group of repeated zero values in an IPv6 address. For example:

2001:DB8::

expands to

2001:0DB8:0000:0000:0000:0000:0000:0000

It is not necessary to supply the leading zeros for a number in an IPv6 address. For example, 2001:DB8::3C:5 is a valid IPv6 address.

BGP

BGP is an inter-AS routing protocol. An AS is a network or a group of devices logically organized and controlled by a common network administration. BGP enables devices to exchange network reachability information. AS paths are the routes to each destination. There are two types of BGP: IBGP and EBGP.

- IBGP is used to communicate with peer devices in the same AS. Routes received from a device in the same AS are not advertised to other devices in the same AS but can be advertised to an EBGP peer.
- EBGP is used to communicate with peers in different ASs. Routes received from a device in a different AS can be advertised to both EBGP and IBGP peers.

See “Inter-AS connections” in section 74.1 for more information about connecting ASs in a VPRN.

You can use the 5620 SAM to enable BGP on the device and perform the following functions:

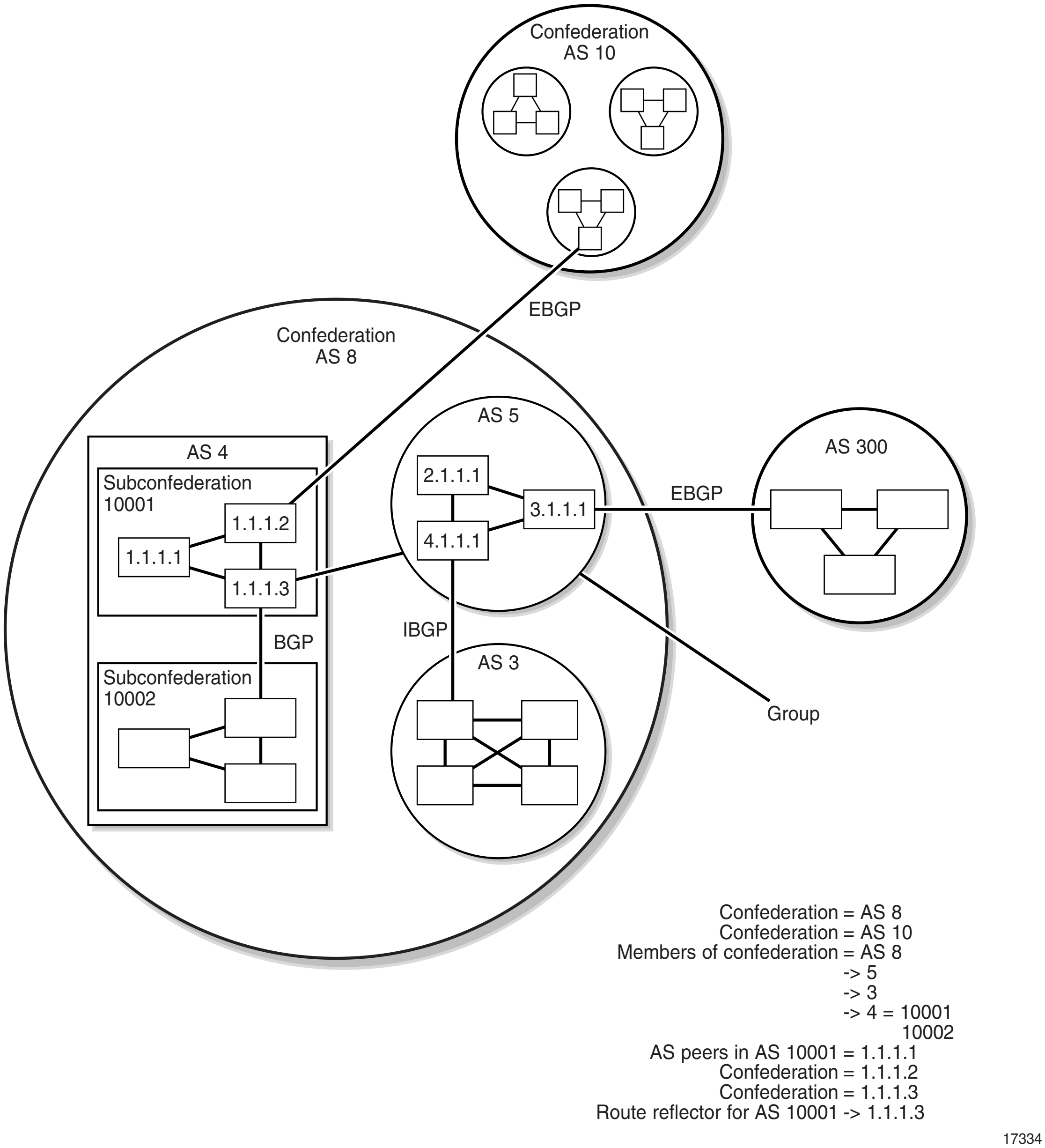
- set the AS values for the routing instance
- create confederations of group-managed devices
- create BGP peer groups
- create neighbors (peers) within the BGP peer groups

The 5620 SAM supports the configuration of IPv6 addresses for BGP peering on the base routing instance of the 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled), and the 7450 ESS in mixed mode.

A device can only belong to one AS. After the neighbor relationship is established between devices, they exchange BGP open messages, which contain information such as AS numbers, BGP versions, router IDs, hold-time values, and keepalive messages. This information determines the status of the BGP session. Peer relationships are defined by configuring the IP addresses of the devices that are peers of the local BGP system.

Figure 31-1 shows a simple BGP example using groups, subconfederations, and confederations.

Figure 31-1 BGP example



In a standard BGP configuration, all BGP-enabled devices within an AS have a full mesh of BGP peerings to ensure all externally learned routes are redistributed through the entire AS. This is needed because IBGP does not re-advertise routes learned from one IBGP peer to another IBGP peer. However, as more devices are added, scaling the IBGP mesh can become an issue. To solve this scaling issue, you can use:

- confederations
- subconfederations

Confederations are a way to subdivide a large AS into smaller ASs. Subconfederations further subdivide ASs. Within each smaller AS, or confederation, IBGP is still used, however EBGP is used between subconfederations. This means less meshing between peers is required.

Another method of subdividing an AS is route reflection. For route reflection, an AS is divided into groups called clusters. Each cluster contains at least one route reflector. The route reflector redistributes routing updates to all devices in its cluster. Because the route reflector provides all the routing updates, the other devices in the cluster do not maintain a BGP mesh.

By default, BGP routers will advertise only the best path to other BGP peers. When the best path fails or a better path is discovered, the old routing information is overwritten. If BGP Add-Path is enabled, peers will advertise multiple paths for the same destination, all of which will be retained in their routing tables. In the event of a failure or path withdrawal message, the router is able to update its forwarding entry for that destination without having to receive new path advertisements. This results in faster convergence after path failure.

MP-BGP

BGP distributes IP routing information between networks. The distribution of IP routing information between VPRNs requires MP-BGP. MP-BGP addressing uses an 8-byte RD with a 4-byte or 16-byte IP address, depending on whether IPv4 or IPv6 is used. The requirements for MP-BGP configuration are the following.

- MP-BGP must be enabled on the participating PE devices.
- All PE devices must be configured as BGP peers.

When PE devices learn routing information from the CE devices in a VPRN configuration, the routing information is shared using MP-BGP. The RD is used to associate the new routing information with a VPRN instance.

The PE devices distribute the route information to the other CE devices in the VPRN. Each learned route is assigned an MPLS label that is distributed to the devices.

When customer packets arrive at a PE device, the packets are encapsulated with the MPLS label that corresponds to the learned route for the packet destination.

The MP-BGP multicast extension can be applied to build separate routing tables for multicast paths. IGPs such as OSPF and IS-IS can import multicast and unicast routing information to the multicast and unicast routing tables. The multicast routing information can subsequently be used by PIM to perform RPF lookups.

RIP

RIP is an IGP that uses a distance-vector algorithm to determine the best route to a destination, using hop count as the deciding factor. In order for the protocol to provide complete information about routing, every device in the domain must participate in the protocol. RIP, a UDP-based protocol, updates its neighbors, and the neighbors update their neighbors.

Unlike OSPF and other link-state protocols, RIP directly advertises reachability information to its neighbors. RIP advertises reachability information by sending prefix, mask, and either hop count or cost metric data. Each device running the RIP protocol advertises all RIP devices periodically by sending RIP update PDUs. The route with the lowest metric is advertised as the best route.

The 5620 SAM supports the configuration of RIPv1 and RIPv2 on network and access interfaces.

The 5620 SAM supports the configuration of IPv6 addresses for RIP on the base routing instance of the 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled).

LDP

LDP is used to distribute labels in non-traffic-engineered MPLS applications. Routers can establish LSPs across a network by mapping network-layer routing information directly to the data link layer switched paths. After the LDP distributes the labels to the LSR, the LSR assigns the label to a FEC, and then informs all other LSRs in the path about the label and how the label switches data accordingly.

A FEC is a collection of common actions associated with a class of packets. LDP helps establish the LSP by providing a set of procedures that LSRs can use to distribute labels.

When a service tunnel is configured on managed routers using LDP signaling in an MPLS environment, LDP sessions are set up based on the configured hello and other PDU values. If another service tunnel is created to the same destination, the LDP session is reused.

The LDP sessions between LSRs:

- find and establish LDP peers in the managed network
- exchange label mappings for each LSR
- exchange label bindings

After all the LSRs are LDP-aware and the LSP is created, forwarding can occur as follows:

1 A FEC is associated with the LSP.

2 The FEC maps the packets to the LSP.

3 The next LSR that is part of the LSP splices incoming FEC labels to the outgoing FEC label of the next hop.

There are two types of LDP:

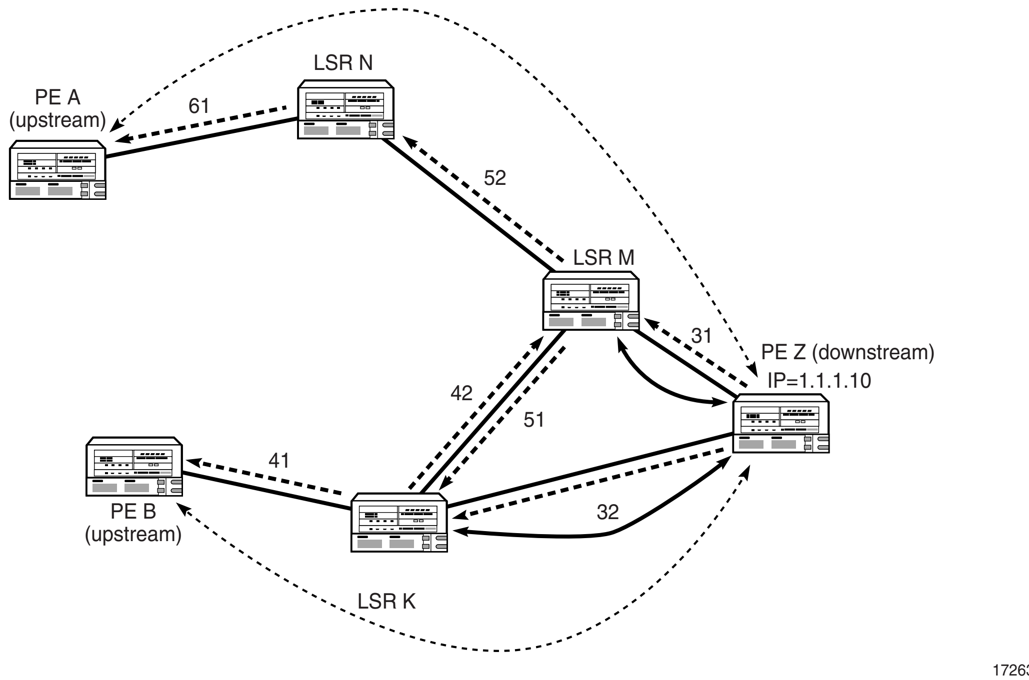
- T-LDP
- DU-LDP

T-LDP is used to distribute labels for VLL and VPLS. T-LDP allows the targeting of remote devices that are not directly connected as targeted peers.

DU-LDP can be used to create tunnels between PEs for IP-VPN services.

Figure 31-2 shows an example of LDPs that are used in a simple Layer 2 and Layer 3 service provider network.

Figure 31-2 LDP sample network



- The solid straight lines between the devices indicate IP connectivity. These are directly connected peers.
- The dotted bidirectional curved lines indicate T-LDP sessions. These are targeted peers that are not directly connected.
- The solid bidirectional curved lines indicate DU-LDP sessions. This example only shows two instances, between M and Z, and Z and K. If there is IP connectivity between all the devices, then all of the devices have DU-LDP sessions.

Provider edge router Z advertises the labels for its address 1.1.1.10 to adjacent link state devices M and K. Routers M and K distribute the labels for that address to the rest of the network.

If provider edge router A wants to send a VPN-labeled packet to router Z, it uses label 61 as the outer label. When the packet reaches router N, outer label 61 is swapped for outer label 52 and the packet continues downstream to router M. Router M then swaps out label 52 for either outer label 31 or 42, depending on router M's label selection algorithm. If outer label 31 is selected, the packet reaches router Z directly, which then continues to route the packet to the customer site based on the VPN label.

If a router receives more than one request for an IP address, and the router does not support ECMP, it selects the first label it receives. If the router supports ECMP, it selects the label with the lowest cost path, or selects both labels if the cost paths are identical.

When a router supports ECMP protocol, LSRs can have multiple equal cost paths to an IP address. ECMP LDP retains all labels it receives from multiple next hop peers. The forwarding plane contains multiple next hops for a FEC and as a result, provides load balancing for LDP-based LSPs.

When a router supports ECMP LDP and a device configured as the next hop is no longer valid, for example a session between peers is lost or the peer withdraws its label, a new valid LDP next hop peer is selected and the forwarding plane is updated.

Load balancing across LSPs for LDP over RSVP is also supported. When ECMP is enabled, all equal cost LSP endpoints are installed in the routing table by the IGP for consideration by LDP. LDP selects the LSP with the lowest LSP metric to determine the next hop. If multiple LSPs are available with equal cost, then ECMP is utilized until the ECMP count is exhausted. An LDP tree is created by sending LSP Trace messages along an ECMP path to downstream LSR nodes.

LDP for P2MP

LDP support for P2MP can be enabled on an LDP interface. You can configure an LDP interface for multicast traffic forwarding towards a downstream node. LDP configuration allows an exchange of P2MP FEC via an established session to a peer, and the use of next hops over an interface.

LDP configuration is supported on a tunnel interface under a base routing instance and under protocols such as PIM and IGMP. A P2MP ID is used as an index for LDP-based tunneling instead of an LSP ID.

Note — BFD and source redundancy are only supported on an RSVP tunnel interface.

IS-IS

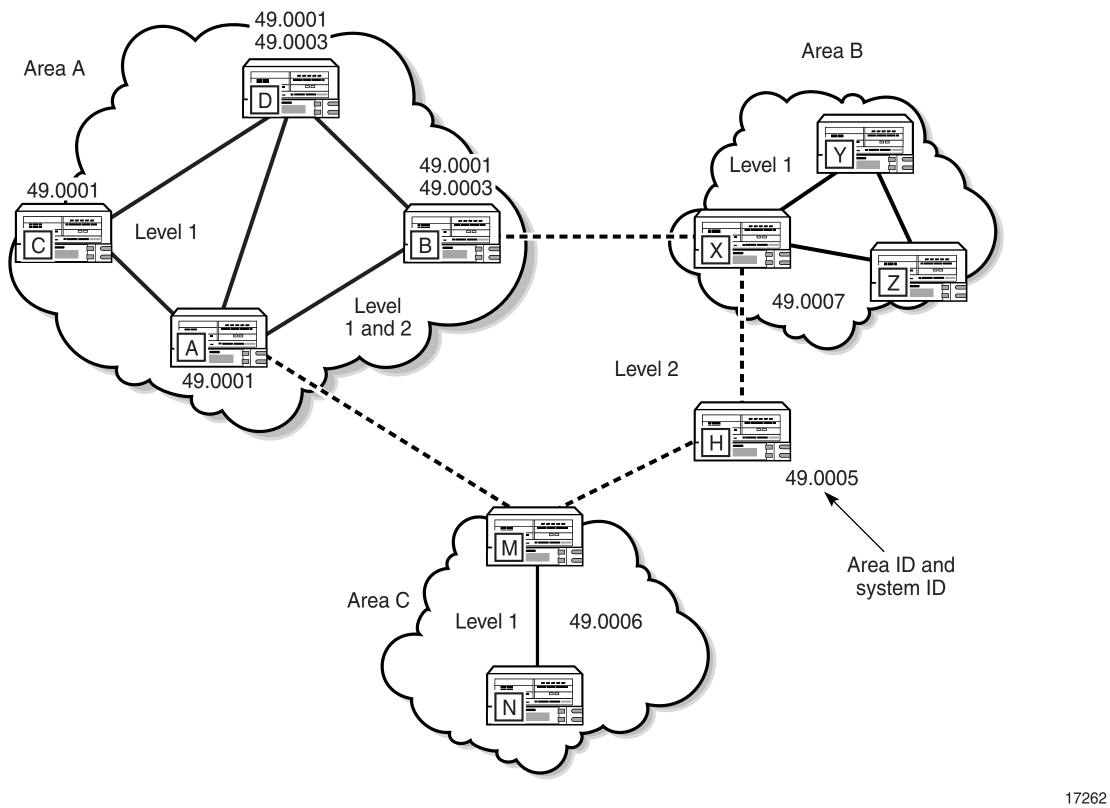
IS-IS is a link-state interior gateway protocol that uses the shortest path first algorithm to determine a route. Routing decisions are made using the link-state information. IS-IS entities include:

- networks, which are autonomous system routing domains
- intermediate systems, which are routers
- end systems, which are network devices that send and receive PDUs

End systems and intermediate system protocols allow devices and nodes to identify each other. The IS-IS protocol sends link state updates periodically through the network, so each device can maintain current network topology information.

Large networks, or autonomous systems, are supported by the IS-IS using a two-level hierarchy. This divides a large area into more manageable, smaller areas. The first level (level 1) of routing is performed within an area. The second level (level 2) of routing is performed between areas, as shown in Figure 31-3.

Figure 31-3 IS-IS routing domains example



Level 2 areas are also called backbones, similar to an OSPF backbone area. All traffic traversing different areas must traverse the backbone.A device can be configured as level 1, level 2, or both level 1 and 2. In this example, routers A, B, M, H, and X form the level 2 IS-IS backbone. The connection between routers A and B carries both level 1 and level 2 link-state PDUs. However, level 1 devices are only aware of their own area's topology, and must forward traffic to a layer 1/2 device to forward the data to another area.

Two devices are in the same level 1 area when they have level 1 adjacency. Level 1 adjacency occurs when the area IDs are common and there is a level 1 connection between the devices. Level 2 adjacency occurs when it has at least one level 1 or 2, or one level 2 interface configured.

The 5620 SAM supports the configuration of IPv6 addresses for IS-IS adjacencies.

Note — If two neighboring devices in the same level 1 area run both level 1 and 2, they establish both a level 1 and level 2 adjacency.

When LDP over RSVP is enabled for IS-IS, LSP can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

After the IS-IS is configured, routing occurs as follows:

1 Hello PDUs are sent to IS-IS-enabled interfaces to discover neighbors and establish adjacencies.
2 IS-IS neighbor relationships are formed.
3 Link-state PDUs are created based on local interfaces and prefixes that are learned from adjacent devices.
4 The devices flood LSPs to adjacent neighbors, and build a link-state database.
5 A shortest path tree is calculated by the IS-IS and the routing table is built.

OSPF

OSPF is a hierarchical link-state interior gateway protocol that operates within ASs and is used in IP networks. OSPF packets are routed based on the destination IP address of the IP packets. Each OSPF router collects link-state information to build a network topology based on OSPF areas. This topology is used to apply the Dijkstra algorithm to calculate the shortest path to each destination in the network. See the appropriate device documentation for more information about OSPF.

When LDP over RSVP is enabled for OSPF, LSP can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

OSPF areas

The hierarchical design of OSPF allows a collection of networks to be grouped into a logical OSPF area. The topology of the area is hidden from the rest of the AS, which significantly reduces OSPF protocol traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely on information obtained within the area; routing information obtained from outside the area is not used. Routers that belong to more than one area called an ABR. An ABR maintains a separate topological database for each area it is connected to. Every router that belongs to the same area has an identical topological database for that area.

OSPF super-backbone

The OSPF super-backbone provides an additional layer of hierarchy in OSPF. The OSPF super-backbone functions include:

- loop prevention
- handling LSAs received from the CE
- managing VPN IPv4 routes received by BGP

The PE routers that connect OSPF areas to the super-backbone function as ABRs in the OSPF areas to which they are attached. To achieve full compatibility, the PE routers can also serve as ASBRs in non-stub areas.

PE routers insert inter-area routes from other areas into the area in which the CE router is present. The CE routers are not involved at any level and are not aware of the super-backbone or other OSPF areas that exist outside of the super-backbone.

When you configure the super-backbone, all destinations that are learned by PEs with matching domain IDs become inter-area routes.

See the appropriate device documentation for more information about the OSPF super-backbone.

RSVP

RSVP is a network control protocol that hosts use to request specific qualities of service from the network for specific data streams. RSVP is also used to deliver QoS requests to all devices in a data path and to establish and maintain the state information required to provide the requested service quality.

RSVP is not a routing protocol. RSVP operates using unicast and multicast routing protocols. RSVP consults local routing tables to relay RSVP messages. By default, RSVP is enabled on all devices that support it.

RSVP requests typically result in the reservation of resources on each device in the data path. MPLS uses this RSVP mechanism to set up traffic-engineered LSPs. RSVP requests resources for unidirectional flows only. RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver.

The RSVP hello protocol detects the loss of a neighbor node or the reset of a neighbor RSVP state information. In standard RSVP, neighbor monitoring occurs as part of the RSVP soft-state model. The reservation state is maintained as cached information that is first installed and then periodically refreshed by the ingress and egress LSRs.

If the state is not refreshed within a specified time interval, the LSR discards the state because it assumes that either the neighbor node has been lost or its RSVP state information has been reset.

Diff-Serv Traffic Engineering support

The 5620 SAM supports Diff-Serv Traffic Engineering, or TE, extensions for RSVP. Diff-Serv TE extensions provide the ability to manage bandwidth in an MPLS network on a per-TE-class basis. With Diff-Serv TE, an LER can perform this on a per-class basis. Therefore, you can set different limits for admission control of LSPs in each TE class over each link in the network.

You do this by setting a bandwidth constraint, which configures the percentage of the RSVP interface bandwidth that each CT shares. The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the Maximum Reservable link bandwidth TE parameter, that is, the link bandwidth multiplied by the RSVP interface subscription parameter.

This configuration also exists at the RSVP interface level and the value specifically configured for the interface overrides the globally-configured value. The bandwidth constraint value can be changed on the fly. You are also allowed to specify the bandwidth constraint for a CT which is not used in any of the TE class definitions and which is not used by any LSP originating or transiting this node.

To enable this feature, in summary, you must:

- configure Diff-Serv Classes on the router RSVP Routing Instances
- configure protocol properties to allow Diff-Serv Classes on the required router RSVP Interfaces
- configure traffic engineering and specify the Class Type that the required dynamic LSPs belongs to
- configure the Diff-Serv Class Type that the required LSP Paths belongs to. This overrides the value set at the LSP level.
- configure Diff-Serv to LSP FC mappings on the required service tunnels (SDPs). User-entered mappings of FC to LSP name are validated automatically (to avoid configuration conflicts) by checking with the RSVP module.

L2TP

L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination point on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated and stopped from either the LNS or LAC.

After an L2TP tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

The 5620 SAM supports the configuration and management of the following:

- ISA-LNS groups
- L2TP sites
- L2TP tunnel group profiles
- L2TP tunnel profiles

ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups on the 7750 SR. ISA-LNS groups provide LNS PPP session termination. An ISA-LNS group is associated with specific L2TP inbound peers and groups. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group.

The following operations can be performed on an ISA-LNS group member:

- drain MDA—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop MDA sessions—terminates the active sessions

See Procedure 18-7 for information about creating and configuring an ISA-LNS group.

L2TP sites

By default, L2TP is enabled on a base routing instance, and an L2TP site is created. An L2TP icon appears in the routing view of the navigation tree. An L2TP site does not exist by default on the base routing instance of a 7450 ESS in non-mixed mode.

L2TP is not enabled by default on a VPRN site. To enable L2TP on a VPRN site, see Procedure 74-1.

L2TP tunnel group profiles

An L2TP tunnel group profile represents the configuration for a group of L2TP tunnels. L2TP tunnel group profiles must be configured on the LNS NE. If a local user database is used on the LAC for session authentication, an L2TP tunnel group profile must be configured on the LAC. When you create an L2TP tunnel group profile, the profile can be used by its child L2TP tunnel profile to inherit certain parameter values. The inherited parameter values are used as the default values during L2TP tunnel profile configuration.

The following operations can be performed on an L2TP tunnel group profile that has a configured L2TP tunnel profile:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes tunnel instances and terminates the active sessions

See Procedure 31-30 for information about managing L2TP tunnel group profiles.

L2TP tunnel profiles

You can create and manage L2TP tunnel profiles from the Tunnel Group Profile properties form.

The following operations can be performed on an L2TP tunnel profile:

- start instance—attempts to create new tunnels
- stop instance—attempts to close the tunnels
- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

See Procedure 31-30 for information about managing L2TP tunnel profiles.

L2TP tunnel instance endpoints

The endpoints of an operational L2TP tunnel are represented by tunnel instance endpoints. You can view tunnel instance endpoints from the Tunnel Instance Endpoints tab on the L2TP Site (Edit) form, and from the Tunnel Group Profile or Tunnel Profile properties form if the endpoint is created using the profile configuration.

An L2TP tunnel instance endpoint is automatically created when:

- a start operation is performed on an L2TP tunnel profile
- an incoming L2TP session is established using group and tunnel profiles
- RADIUS authentication returns a configuration for the tunnel when an incoming L2TP session is authenticated and PPP session authentication determines that L2TP is used, at which point an L2TP session is established.

The following operations can be performed on an L2TP tunnel instance endpoint:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes the tunnel instances and terminates the active sessions

L2TP peers

An L2TP site can have none or multiple L2TP peers. L2TP peer information is available on the Peers tab of the L2TP Site form. Information about L2TP tunnels for a specific L2TP peer is available on the Tunnels tab of the L2TP Peer properties form.

The following operations can be performed on an L2TP peer:

- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

L2TP tunnels and tunnel endpoints

You can view information about L2TP tunnels and tunnel endpoints from the L2TP Tunnel - Endpoint A - Endpoint B form. See Procedure 31-31 for information about viewing L2TP tunnels and tunnel endpoints.

PIM

PIM is a component of multicast routing that defines the one-to-many or many-to-many transmission of information. You can use the following variations for PIM configurations:

- sparse mode
- dense mode
- source-specific multicast
- bidirectional

Sparse mode is the most common PIM configuration. Sparse mode is used for data transmission to nodes in multiple Internet domains that contain a small ratio of nodes that subscribe to the multicast traffic. Dense mode is used when a large ratio of the potential nodes subscribe to the multicast traffic. In source-specific multicast, paths originate at a single, defined source. Bidirectional PIM is not source-specific.

Anycast RP

Anycast RP for PIM-SM enables fast convergence when a PIM RP router fails. The receivers and sources rendezvous at the closest RP after the router failure. Anycast RP allows an arbitrary number of RPs for each group in a single, shared-tree PIM-SM domain. Triple play configurations that distribute multicast traffic using PIM-SM realize the benefits of fast RP convergence, which helps to avoid the loss of multicast data streams or IPTV delivery to the end user.

Anycast RP for PIM-SM environments is supported in the base routing PIM-SM instance of the service router. The 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support Anycast RP in VPRN instances that are configured with PIM.

Anycast RP for PIM requires the completion of the following configuration information:

- An IP address specified as the RP address. This address is statically configured, or distributed using a dynamic protocol, to all PIM routers in the domain.
- A set of routers in the domain designated as RPs for the RP address. These routers form an anycast RP.
- Each of these routers is configured with a loopback interface that uses the RP address. The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the anycast RP also needs a separate IP address, to be used for communication between the RPs.
- Each router in the anycast RP is configured with the addresses of all other routers in the anycast RP. The addresses must be consistently configured in all RPs in the set.

Figure 31-4 shows a sample implementation of anycast RP for PIM-SM.

Figure 31-4 Sample implementation of anycast RP for PIM-SM

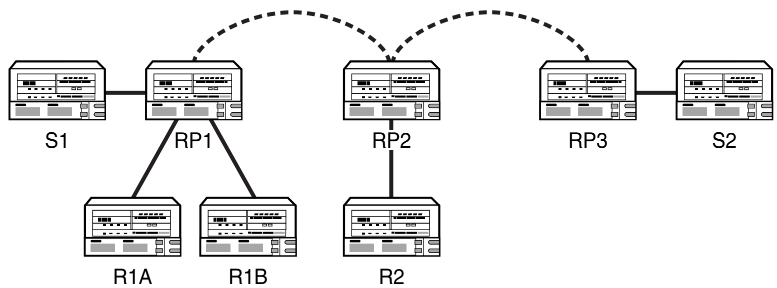


Table 31-1 summarizes the sequence of events for the Anycast RP implementation shown in Figure 31-4.

Table 31-1 Sequence of events for Anycast RP fast convergence

Sequence	Event description
1	S1 sends a multicast packet.
2	The router connected to S1 forms a PIM registration message to send to the Anycast RP address. The unicast routing system delivers the PIM registration message to the nearest RP, in this case RP1.
3	RP1 receives the PIM registration message, decapsulates the message, and sends the packet down the shared tree to the R1A and R1B receivers.
4	RP1 is configured with the IP address for RP2 and RP3. Since the registration message did not come from one of the RPs in the anycast RP set, RP1 assumes that the packet came from a designated router.
5	RP1 sends a copy of the registration message from the S1 designated router to RP2 and RP3. RP1 uses its own IP address as the source address for the PIM registration message.
6	RP1 can join the source tree by sending a join message to S1. However, RP1 must create a source-specific state.
7	RP2 receives the registration message from RP1, decapsulates the message, and send the packet down the share tree to the R2 receiver.
8	RP2 sends a registration-stop message back to RP1. RP2 can wait to send the registration-stop message if it decides to join the source tree. RP2 should wait until it receives data from the source tree before it sends the registration-stop message. If RP2 does wait for the data, the registration-stop message is sent to RP1 when it receives the next registration message. If RP2 does not wait for the data, the registration-stop message is immediately sent to RP1.
9	RP2 can join the source tree by sending a join message to S1. However, RP2 must create a source-specific state.
10	RP3 receives the registration message from RP1 and decapsulates the message. No receivers joined for the group, so RP3 discards the packet.
11	RP3 sends a registration-stop message back to RP1.

(1 of 2)

Sequence	Event description
12	RP3 creates a source-specific state, so when a receiver joins after S1 starts sending traffic, RP3 can quickly join the source tree for S1.
13	RP1 processes the registration-stop message from RP2 and RP3. RP1 can cache the receipt of registration-stop messages from the RPs in the anycast RP set. (The cache of messages is completed on a per-RP or per-source-specific basis.) The cache of messages increases the reliability of the delivery of registration messages to each RP. Subsequent registration messages received by RP1 are sent only to the RPs in the anycast RP set that have not previously sent registration-stop messages from the source-specific entry.
14	RP1 sends a registration-stop message to the DR under the following conditions: • after receiving a registration message from the DR • if all RPs in the anycast RP set have returned registration-stop messages for a specific source-specific route

(2 of 2)

SPT switchover thresholds

SPT switchover thresholds allow you to configure the switchover threshold, in Kbps, for the group prefixes. The threshold value determines when the router switches from the shared tree to the source-specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.

L3 Multicast Load Balancing for ECMP

The 5620 SAM distributes multicast traffic by balancing the load based on the total available multicast bandwidth on all ECMP paths. You can configure ECMP rebalancing on the VPRN and base PIM Routing Instance configuration forms.

5620 SAM ECMP rebalancing has the following important characteristics:

- Multicast load balancing over ECMP links is enabled, by default.
- The rebalancing timer is set to 30 minutes, by default.
- Distribution of the multicast groups over the available links is processed based on the bandwidth configured for the specified group address. If the bandwidth is not configured for the multicast stream, then the configured default value is used.
- If a link failure occurs, the load on the failed channel is distributed to the remaining channels. The bandwidth required to accommodate the load from the failed link is evenly distributed over the remaining links.
- If an additional link becomes available for a specific multicast channel, it is then treated in an equivalent manner to the other links of the interface.
- A manual (operator-initiated) rebalance command is typically used to re-evaluate the current balance, with regard to bandwidth utilization. If necessary, multicast streams can subsequently be moved to different links to achieve a balance.
- In an automatic timed rebalance, the system rebalances multicast streams over the available links, based on the configured bandwidth and interval. If no links have been added or removed, or it is determined that no multicast streams will benefit from a rebalance, then it is not be implemented.

- When multicast load rebalancing is not enabled, any ECMP changes are not optimized. However, whenever a link is added, an attempt is made to balance the number of multicast streams on all the available ECMP links. This may however, not result in balanced bandwidth utilization of all the ECMP links.
- Only a single rebalance command can be executed at any specific time. If a rebalance is in progress and a manual rebalance command is entered, it is rejected and a message is displayed informing the user that a rebalance is already in progress.

IGMP

IGMP is a multicast protocol which service providers can use to establish multicast group memberships on a LAN. Within the LAN, end users use IGMP to communicate with a local multicast router, which then uses PIM to distribute the IGMP messages to other local and remote multicast routers. Multicast routers send regular membership queries to IGMP hosts which respond with membership reports. Multicast routers can use these reports to determine which hosts are interested in receiving particular multicast messages.

IGMP operates above the network layer on IPv4 networks.

MSDP

MSDP is a protocol that enables multiple PIM-SM domains to communicate with each other using their own RPs. MSDP also enables multiple RPs in a single PIM-SM domain to establish MSDP mesh-groups and to synchronize information between anycast RPs about the active sources being served by each anycast RP peer. The 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support MSDP.

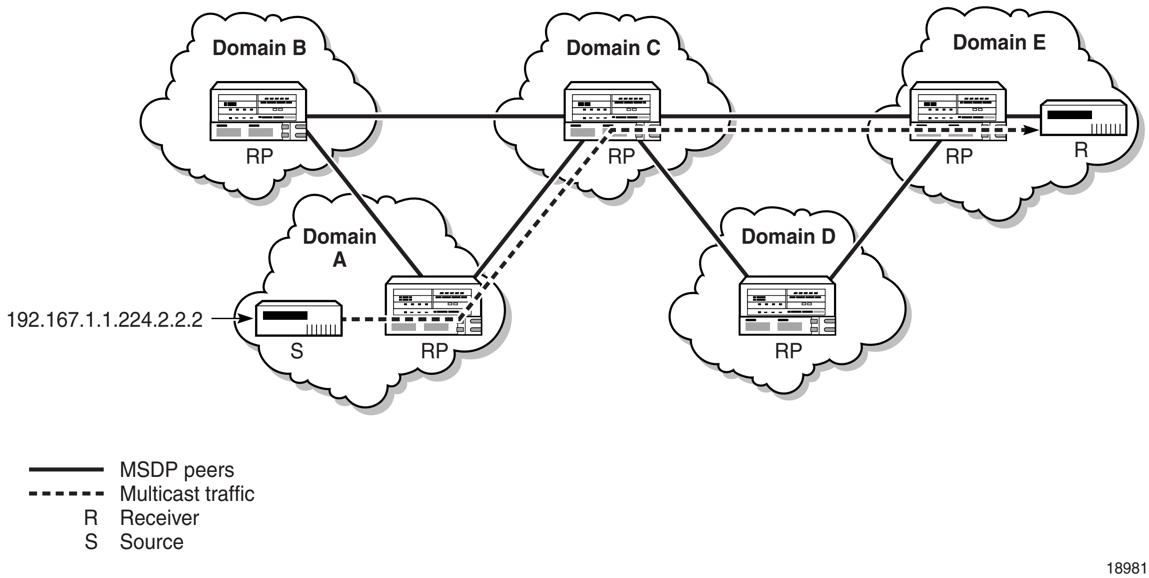
Each PIM-SM domain has its own RPs and MSDP enables these RPs to inform each other about active sources. When an active source is detected, the RPs send PIM-SM explicit join messages to the active source. When RPs in remote domains know about active sources, they can pass on this information to their local receivers and multicast data can be forwarded between the domains.

The RP learns about a new multicast source within its own domain through the PIM register mechanism and encapsulates the first data packet in a source active message. After an RPF check, the MSDP source active message is flooded by each peer to its MSDP peers until it reaches every MSDP router in the interconnected networks. If the receiving MSDP peer is an RP, and the RP has a (*,G) entry for the group in the source active message, the message is accepted. The RP creates an (S,G) state for the source and join to the shortest path tree for the state of the source.

The encapsulated data is forwarded down the RP's shared tree. When the packet is received by a receiver's last hop router, the last-hop may also join the shortest path tree to the source.

Figure 31-5 shows a sample of how data flows from a source in Domain A to a receiver in Domain E in an MSDP implementation for PIM-SM.

Figure 31-5 Sample implementation of MSDP for PIM-SM



MLD

MLD is an asymmetric protocol used by IPv6 routers to discover the presence of multicast listeners, that is, nodes that wish to receive multicast packets. MLD specifies separate behaviors for multicast address listeners and multicast routers.

The purpose of MLD is to enable each multicast router to discover, for each of its directly attached links, which multicast addresses and which sources have interested listeners on that link. The information gathered by MLD is provided to whichever multicast routing protocol is used by the router, such as PIM, to ensure that multicast packets are delivered to all links where there are listeners interested in such packets.

MLD is supported on a chassis mode C or D, and on the 7750 SR in chassis mode A or B with mixed mode enabled.

Bridging

Bridging is used between a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device and a 7450 ESS to create a fast ring that bridges the end-user devices, such as BTV set-top boxes, and Layer 2 services, such as VPLS, that distribute multicast traffic. If required, you can configure the devices with MSTP or another STP.

STP is active by default on an OmniSwitch. The default mode of operation is 1x1 mode using RSTP. A loop-free network topology is automatically calculated based on default STP switch, bridge, and port parameter values.

Additional OmniSwitch configuration such as enabling and configuring OmniSwitch learned port security parameters for VLAN ports, DHCP relay, and DHCP snooping can be done while configuring other bridge parameters.

You can configure Multiple VLAN Registration Protocol (MVRP) as part of the bridging configuration on some versions of the OmniSwitch. MVRP provides a mechanism to maintain the contents of dynamic VLAN registration entries for each VLAN, and to propagate that information to other bridges.

In the 5620 SAM, a bridge is represented in the network view below a device, similar to the routing instance of a device.

31.2 Workflow to configure protocols

This workflow assumes the following:

- You know the 32-bit unique router ID prior to configuring OSPF or BGP.
- An AS number is assigned to the device prior to configuring BGP.

1 Enable the routing protocols to be supported on the devices. See the appropriate device documentation for more information. The options are:

- LDP
- IS-IS
- MPLS
- RSVP (enabled by default)
- BGP
- RIP
- L2TP (enabled by default)
- OSPFv2
- OSPFv3
- PIM
- IGMP
- MSDP
- MLD

Note — L2TP is enabled by default on a base routing instance, but not on a VPRN routing instance.

2 Ensure the parameters to implement routing protocols on the Layer 3 interfaces are configured. See chapter 30 for more information.

3 As required on the selected routing protocol, configure routing policies. See chapter 30 for more information.

4 Review the appropriate workflow to configure a routing protocol:

a BGP; see section 31.3 for more information

b RIP; see section 31.4 for more information

c LDP; see section 31.5 for more information

d IS-IS; see section 31.6 for more information

e OSPFv2 or OSPFv3; see section 31.7 for more information

f RSVP; see section 31.8 for more information

g L2TP; see section 31.9 for more information

h PIM; see section 31.10 for more information

- **i** IGMP; see section 31.11 for more information
- **j** MSDP; ee section 31.12 for more information
- **k** MLD; see section 31.13 for more information
- **l** bridging; see section 31.14 for more information

5 As required, configure the protocol for the remote device.

31.3 Workflow to configure BGP

1 Enable BGP on the routing instance. See Procedure 31-1 for more information.

2 Determine whether BGP confederations are necessary. If BGP confederations are necessary:

- **a** Configure the Confederation Autonomous System number on the Routing tab of the Routing Instance configuration form.
- **b** Configure BGP confederation members from the BGP Confederations tab of the Routing Instance configuration form. See Procedure 31-3 for more information.

3 If you are configuring MP-BGP, perform the following on the base routing instance of each NE that is to participate in a VPRN:

- **a** As required, enable VPN IPv4 and VPN IPv6.
- **b** As required, enable multicast IPv4 to apply the multicast extension. See Procedure 31-2 and chapter 74 for more information.

4 Create at least one BGP peer group. See Procedure 31-4 for more information.

5 As required, create BGP neighbors with which to peer. See Procedure 31-5 for more information.

6 As required, enable or disable BGP peering. See Procedure 31-6 for more information.

31.4 Workflow to configure RIP

1 Enable RIP on the routing instance. See Procedure 31-7 for more information.

2 Configure global-level RIP. See Procedure 31-8 for more information.

3 Configure group-level RIP. See Procedure 31-9 for more information.

4 Configure neighbor-level (also known as interface) RIP. See Procedure 31-10 for more information.

31.5 Workflow to configure LDP

1. Enable LDP on the routing instance. See Procedure 31-11 for more information.
2. Configure global-level LDP. See Procedure 31-12 for more information.
3. Configure one of the following options.
   a. If two LDP peers are adjacent devices, create an LDP interface. See Procedure 31-13 for more information.
   b. If two LDP peers are non-adjacent devices, create an LDP targeted peer. See Procedure 31-14 for more information.
4. As required, configure ECMP on an LDP routing interface. See Procedure 31-16 for more information.
5. Create an LDP keychain. See Procedure 31-15 for more information.

31.6 Workflow to configure IS-IS

1. Enable IS-IS on the routing instance. See Procedure 31-17 for more information.
2. Configure global-level IS-IS. See Procedure 31-18 for more information.
3. Configure at least one NET address. See Procedure 31-19 for more information.
4. Configure at least one IS-IS interface. See Procedure 31-20 for more information.
5. As required, if LDP over RSVP is enabled for IS-IS, configure an operational LSP between routers. See chapter 32 for more information.

31.7 Workflow to configure OSPFv2 and OSPFv3

1. Enable OSPF on the routing instance. See Procedure 31-21 for more information.
2. Configure OSPF on the routing instance. See Procedure 31-22 for more information.
3. Create at least one OSPFv2 or OSPFv3 area. See Procedure 31-23 for more information.
4. Assign routers to the OSPFv2 or OSPFv3 area. See Procedure 31-24 for more information.
5. Assign Layer 3 interfaces to the routers in the OSPFv2 or OSPFv3 area. See Procedure 31-25 for more information.
6. As required, create an OSPF area range. See Procedure 31-26 for more information.
7. As required, create a virtual link between the backbone OSPF area and a remote OSPF area that does not advertise the OSPF topology. See Procedure 31-27 for more information.

31.8 Workflow to configure RSVP

1. As required, configure MPLS, LSP, MPLS path, and LSP path parameters. See chapter 32 for more information.
2. Configure the RSVP on the routing interface. See Procedure 31-28 for more information.
3. Configure the RSVP interface. See Procedure 31-29 for more information.
4. As required, enable LDP. See Procedure 31-11 for more information.

31.9 Workflow to configure L2TP

1. Configure L2TP on a routing instance. See Procedure 31-30 for more information.
2. Create and configure an LNS group and group member for an LNS site. If the site is a LAC, this configuration is not required. See Procedure 18-7 for more information.
3. As required, configure the ESM profiles for LNS L2TP termination:
   - **a** VPRN; see Procedure 74-13 for more information
   - **b** IES; see Procedure 73-8 for more information
4. As required, configure L2TP on each local user database PPPoE host to be forwarded to the LNS (applicable for the LAC and the LNS, where RADIUS is not used). See Procedure 68-32 for more information.
5. As required, view L2TP tunnels and endpoints. See Procedure 31-31 for more information.

31.10 Workflow to configure PIM

1. Enable PIM on a routing instance. See Procedure 31-32 for more information.
2. Configure PIM on a routing instance. See Procedure 31-33 for more information.
3. As required, configure Anycast RP for PIM on a router. See Procedure 31-34 for more information.
4. Configure a PIM interface. See Procedure 31-35 for more information.

31.11 Workflow to configure IGMP

1. Enable IGMP on the routing interface. See Procedure 31-36 for more information.
2. Configure IGMP on the routing instance.See Procedure 31-37 for more information.
3. As required, configure IGMP on an OmniSwitch. See Procedure 31-38 for more information.

4 Configure an IGMP interface. See Procedure 31-39 for more information.

5 As required, turn up or shut down an IGMP interface. See Procedure 31-40 for more information.

6 As required, view IGMP statistics, as follows:

  a IGMP multicast reporting statistics; see Procedure 31-41 for more information

  b IGMP source statistics; see Procedure 31-42 for more information

31.12 Workflow to configure MSDP

1 Enable MSDP on the routing instance. See Procedure 31-43 for more information.

2 Configure global MSDP on the routing instance. See Procedure 31-44 for more information.

3 Create at least one MSDP peer or group-peer.

  a As required, configure group-level MSDP. See Procedure 31-45 for more information.

  b As required, configure peer-level MSDP. See Procedure 31-46 for more information.

4 As required, configure group-peer-level MSDP. See Procedure 31-48 for more information.

5 As required, configure an MSDP source. See Procedure 31-47 for more information.

6 As required, enable or disable MSDP peering. See Procedure 31-49 for more information.

31.13 Workflow to configure MLD

1 Enable MLD on the routing instance. See Procedure 31-50 for more information.

2 Configure MLD on the routing instance. See Procedure 31-51 for more information.

3 Create an MLD interface. See Procedure 31-52 for more information.

31.14 Workflow to configure bridging on a 7250 SAS or Telco device

1. As required, configure bridging on a 7250 SAS or Telco device. See Procedure 31-53 for more information.
2. As required, configure bridging on an OmniSwitch. See Procedure 31-54 for more information.
3. As required, release a violated OmniSwitch LSP port. See Procedure 31-55 for more information.

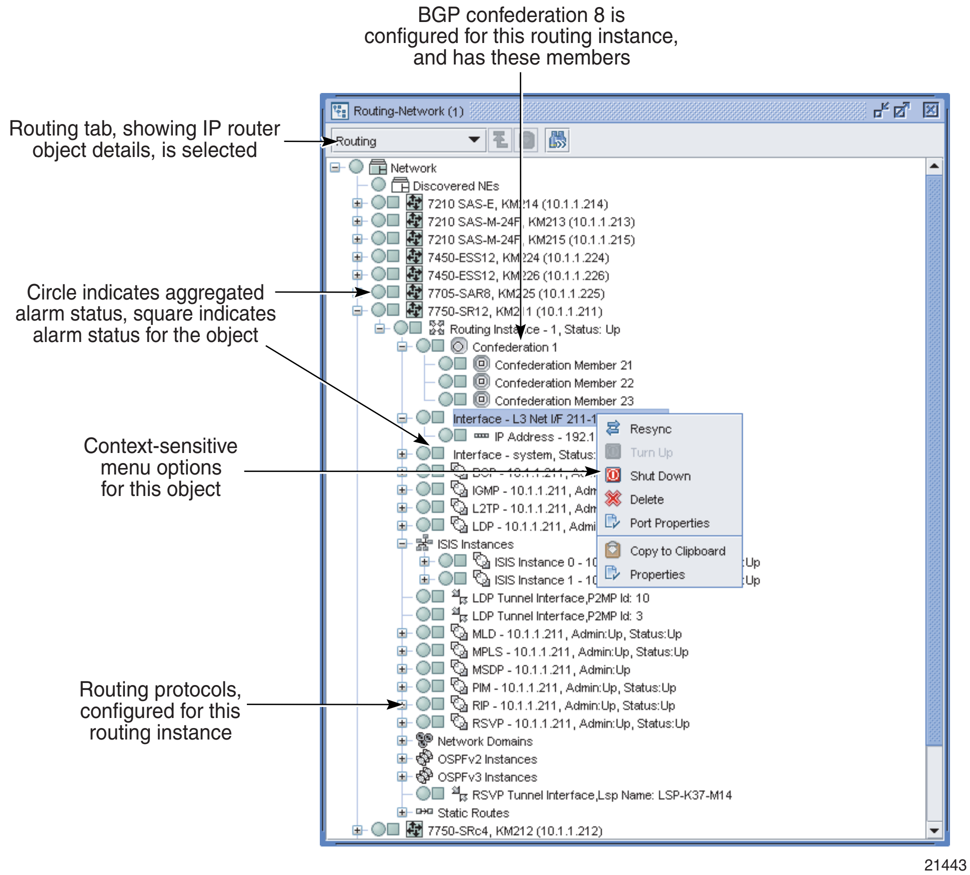
31.15 BGP configuration procedures

The BGP command hierarchy consists of three levels:

- global
- peer group
- peer (also known as neighbor)

Figure 31-6 shows the network view open to show Confederations and BGP settings.

Figure 31-6 BGP in the navigation tree network view



BGP parameters are initially applied at the global level. These parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical BGP commands can be modified at different levels. BGP group-level parameters take precedence over BGP global-level parameters. BGP peer-level parameters take precedence over group- and global-level parameters.

The following procedures describe how to configure BGP.

Procedure 31-1 To enable BGP on a routing instance

1. From the 5620 SAM GUI, choose Routing from the navigation tree view selector.
2. Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.
3. Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Enable BGP.

i Click on the Protocols tab button.

ii Choose the BGP Enabled parameter.

Note 1 — You must configure an AS number before enabling BGP. Configure the Autonomous System parameter on the Routing tab of the Routing Instance (Edit) form.

Note 2 — If a confederation is required, configure the Confederation Autonomous System parameter on the Routing tab on the Routing Instance (Edit) form.

5 Click on the OK button. The Routing Instance (Edit) form closes, a BGP entry appears in the list of enabled protocols, and a BGP icon appears in the network view of the navigation tree.

Procedure 31-2 To configure global-level BGP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the BGP icon. The path is Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Properties. The BGP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Router ID
- Administrative State
- Cluster ID

5 Configure the parameters in the MED block:

- MED Compare
- MED Source
- MED Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

6 Configure the parameters in the MultiPath block:

- Multi Path
  Set to 1 to disable. When set from 2 to 16, multipath is enabled and BGP load shares traffic across the number of links specified. If the equal cost routes available are greater than the configured value, then routes with the lowest next hop IP address are chosen.
- IBGP MultiPath
- EIBGP LoadBalance

7 Configure the Backup Path parameter in the Backup Path block.

8 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the Select button in the KeyChain block. The Select BGP Site Keychain - BGP form opens.

ii Select a key chain in the list and click on the OK button. The Select BGP Site Keychain - BGP form closes. The 5620 SAM assigns the key chain to the BGP instance.

9 If you are configuring BGP for a VPRN routing instance, go to step 12.

10 Configure the parameters in the Graceful Restart block:

- Graceful Restart
- Stale Routes Time (seconds)

The Stale Routes Time (seconds) parameter is configurable when the Graceful Restart parameter is enabled.

The Graceful Restart parameter is not configurable on 7210 SAS-M and 7210 SAS-X devices.

11 Configure the parameters in the IGP Shortcut block:

- IGP Shortcut
- Disallow IGP

The Disallow IGP parameter is only displayed if you enable one of the IGP Shortcut options.

12 Click on the Behavior tab button.

13 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- FlowSpec Validate Enabled
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Inter AS VPRN
- Enable Rapid Withdrawal
- Enable Peer Tracking
- BFD Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Purge Time (minutes)
- Transport Tunnel
- Path MTU Discovery Enabled
- Hold Time (seconds)
- Enable Add-Path Send
- Add-Path Receive
- IPv4 Add-Path Limit
- VPN IPv4 Add-Path Limit
- IPv6 Add-Path Limit
- VPN IPv6 Add-Path Limit

The Enable Inter AS VPRN parameter is not configurable on a VPRN routing instance.

14 Click on the AS Properties tab button.

15 Configure the parameters:

- Min AS Origination (seconds)
- Disable 4Byte ASN
- Local AS
- Private
- Remove Private AS
- Limited

The Local AS parameters are used to configure a virtual AS. A virtual AS is used when a router (RTA) is moved from one AS (AS1) to another AS (AS2). However, the customer router (CR1) is configured to belong to the AS1. To avoid reconfiguring CR1 to belong to AS2, CR1 can continue to belong to AS1, but RTA has its local AS value set to AS1. RTA can advertise AS1 for routes advertised to CR1.

16 Click on the VPN tab button.

17 Configure the parameters:

- Family
- Apply Import Route Policies
- Apply Export Route Policies
- AS Override
- AS Path Ignore Family

If you are configuring global-level BGP for BGP AD in VPLS or for BGP VPLS, then you must enable L2 VPN in the Family block.

The Apply Import Route Policies and Apply Export Route Policies parameters are not configurable on a VPRN routing instance.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

18 Configure the Address Family parameter in the Rapid Update block.

19 Configure the Address Family parameter in the Advertise External block.

20 Perform the following steps to add a peer group, if required.

i Click on the Group tab button.

ii Click on the Create button.The Peer Group (Create) form opens.

iii Perform steps 4 to 20 of Procedure 31-4.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer Group (Create) form closes.

21 Perform the following steps to add a peer, if required.

i Click on the Peer tab button.

ii Click on the Create button. The Peer (Create) form opens.

iii Perform steps 4 to 21 of Procedure 31-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

22 Click on the Import Policies tab button.

23 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

24 Click on the Export Policies tab button.

25 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. A router performs no validation to ensure the policies match.

26 Click on the Authentication tab button.

27 Configure the parameters:

- Type
- Key

28 Click on the following tab buttons to view information:

- Statistics
- Faults

29 Click on the OK button. The BGP (Edit) form closes.

Procedure 31-3 To configure a BGP confederation

For BGP confederations, the following rules apply:

- A device can only belong to one confederation.
- Multiple devices can belong to one BGP confederation.

You must configure BGP on the device and configure global-level BGP parameters before you configure BGP confederations, as described in Procedures 31-1 and 31-2.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the Routing Instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Routing tab button.

5 Enter the confederation number for the Confederation Autonomous System parameter and click on the Apply button.

6 Click on the BGP Confederations tab button.

7 Click on the Create button to add a BGP confederation, or select a BGP confederation from the list and click on the Properties button to configure an existing BGP confederation. The Confederation (Edit) form opens with the General tab displayed.

Note — You can only have one BGP confederation per device.

8 To add a new member to the confederation:

i Click on the Members tab button.

ii Click on the Create button. The Confederation Member (Create) form opens.

iii Configure the Member AS parameter as the number of ASs for the confederation. The member AS number represents the BGP instance of the device.

iv Click on the OK button. The Confederation Member (Create) form closes, and an entry for the new confederation member AS appears in the Confederation (Edit) form.

9 Click on the OK button. The Confederation (Edit) form closes and the Routing Instance (Edit) reappears. A Confederation icon appears in the Navigation Tree below the Routing Instance icon.

You can verify the confederation membership by opening the Confederation icon to view icons that represent the members of the confederation as specified in step 8.

10 Close the Routing Instance (Edit) form.

Procedure 31-4 To configure peer-group-level BGP

Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the global-level BGP configuration is set to True, the only available option for the same parameter in the peer-group-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer group take precedence over the parameters that are configured for global-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the BGP icon by choosing Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Create Group. The Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Administrative State
- Cluster ID
- Local Address
- Inherit Value
- Dynamic Peer

5 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the Select button in the KeyChain block. The Select BGP Group Keychain - Peer Group form opens.

ii Select a key chain in the list and click on the OK button. The Select BGP Group Keychain - Peer Group form closes. The 5620 SAM assigns the key chain to the BGP peer group.

6 Configure the parameters in the Graceful Restart block:

- Graceful Restart
- Stale Routes Time (seconds)
- Inherit Value

The Stale Routes Time (seconds) parameter is configurable when the Graceful Restart parameter is enabled.

The Graceful Restart parameter is not configurable on 7210 SAS-M and 7210 SAS-X devices.

7 Configure the parameters in the MED block:

- MED Source
- MED Value
- Inherit Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

8 Click on the Behavior tab button.

9 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Peer Tracking
- BFD Enabled
- FlowSpec Validate Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Path MTU Discovery Enabled
- Hold Time (seconds)
- Prefix Limit
- Prefix Limit Log Only
- Prefix Limit Threshold
- Enable Add-Path Send
- Add-Path Receive
- IPv4 Add-Path Limit
- VPN IPv4 Add-Path Limit
- IPv6 Add-Path Limit
- VPN IPv6 Add-Path Limit
- Inherit Value

10 Click on the AS Properties tab button.

11 Configure the parameters:

- Peer AS
  The parameter specifies the peer AS for this specific group, and the behavior, either internal or external. Multipath configurations are not supported at the BGP peer level.
- Min AS Origination (seconds)
- Disable 4Byte ASN
- AS Override
- Local AS
- Private
- Remove Private AS
- Limited
- Inherit Value

12 Click on the VPN tab button.

13 Configure the parameters:

- Family
- Advertise Label
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value

Note 1 — The Advertise Label, Apply Import Route Policies, and Apply Export Route Policies parameters are not configurable for a VPRN routing instance.

Note 2 — The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

14 Perform the following steps to add a peer, if required.

i Click on the Peer tab button.

ii Click on the Create button. The Peer (Create) form opens.

iii Perform steps 4 to 21 of Procedure 31-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

15 Click on the Import Policies tab button.

16 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

17 Click on the Export Policies tab button.

18 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Note — Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. A router performs no validation to ensure the policies match.

19 Click on the Authentication tab button.

20 Configure the parameters:

- Type
- Key
- Inherit Value

21 Click on the following tab buttons to view information.

- Statistics
- Faults

22 Click on the OK button. The Peer Group (Create) form closes, and the 5620 SAM displays an icon for the new peer group under the BGP icon in the navigation tree.

Procedure 31-5 To configure peer-level BGP

Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the peer-group-level BGP configuration is set to True, the only available option for the same parameter in the peer-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer take precedence over the parameters that are configured for group-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to a peer group by choosing Routing→Router→Routing Instance→BGP→Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- Description
- Administrative State
- Cluster ID
- Local Address
- Inherit Value

5 Click on the Behavior tab button.

6 Configure the parameters:

7 Click on the AS Properties tab button.

8 Configure the parameters:

- Peer AS
  The parameter specifies the peer AS for the group to which the peer belongs, and the behavior, either internal or external. Multipath configurations are not supported at the BGP peer level.
- Local AS
- Private
- Remove Private AS
- Limited
- Min AS Origination (seconds)
- Disable 4Byte ASN
- Inherit Value

9 Click on the MED tab button.

10 Configure the parameters:

- MED Source
- MED Value
- Inherit Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

11 Click on the VPN tab button.

12 Configure the parameters:

- Family
- Advertise Label
- Advertise LDP Prefix
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value

The Advertise LDP Prefix is only displayed when the Advertise Label parameter is enabled for IPv4 routes.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

13 Click on the Graceful Restart tab button.

14 Configure the parameters:

- Graceful Restart
- Stale Routes Time (seconds)
- Inherit Value

15 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select BGP Peer Keychain - Peer form opens.

iii Select a key chain in the list and click on the OK button. The Select BGP Peer Keychain - Peer form closes and the 5620 SAM assigns the key chain to the BGP peer.

16 Click on the Import Policies tab button.

17 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

18 Click on the Export Policies tab button.

19 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 30. A router performs no validation to ensure the policies match.

20 Click on the Authentication tab button.

21 Configure the parameters:

- Type
- Key
- Inherit Value

22 Click on the OK button. The Peer (Create) form closes and a Peer icon appears below the Peer Group icon in the Navigation Tree of the network view.

23 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 31-6 To enable or disable BGP peering

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to a peer group by choosing Routing→Router→Routing Instance→BGP→Peer Group.

3 Click on the Peer Group icon to display the peers in the peer group.

4 Right-click on a peer and choose one of the following menu items:

   a Turn Up to activate a peer

   b Shut Down to deactivate a peer

5 A dialog box appears. Click on the Yes button. The state information beside the Peer icon changes accordingly.

31.16 RIP configuration procedures

The RIP command hierarchy consists of three levels:

- global
- group
- interface (also known as neighbor)

For RIP configuration, you must define at least one group and one interface. The parameters that are configured on the global level are inherited by the group and interface levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical RIP commands can be modified on different levels. RIP group-level parameters take precedence over BGP global-level parameters. RIP interface-level parameters take precedence over peer-group and global-level parameters.

The following procedures describe how to configure RIP.

Procedure 31-7 To enable RIP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable RIP.

   i Click on the Protocols tab button.

   ii Select the RIP Enabled parameter.

5 Click on the OK button to save the changes. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and a RIP icon appears under the routing instance in the navigation tree.

Procedure 31-8 To configure global-level RIP

1. Choose Routing from the navigation tree view selector from the 5620 SAM GUI.
2. Navigate to the RIP icon by choosing Routing→Router→Routing Instance→RIP.
3. Right-click on the RIP icon and choose Properties. The RIP Site (Edit) form opens with the General tab displayed.
4. Configure the parameters:
   - Description
   - Administrative State
5. Click on the Behavior tab button.
6. Configure the parameters:
   - Check Zero
   - Message Size
   - Metric In
   - Metric Out
   - Preference
   - Receive
   - Send
     The parameter specifies the type of messages received based on the RIP version, and the variation of RIPv2 messages sent, either broadcast or multicast.
   - Split Horizon
   - Propagate RIP Metric
     This parameter is configurable only when configuring RIP on a VPRN routing instance.
   - Flush
   - Timeout
   - Update
7. Click on the Authentication tab button.
8. Configure the parameters:
   - Type
   - Key
9. Click on the Import Policies tab button.
10. Configure the parameters:
    - Policy 1
    - Policy 2
    - Policy 3
    - Policy 4
    - Policy 5

Specify routing policies that determine the routes that RIP interfaces import. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

11 Click on the Export Policies tab button.

12 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Specify routing policies that determine the routes that RIP interfaces export. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

13 To create a RIP group, click on the Group tab button.

i Click on the Create button. The RIP Group (Create) form opens.

ii Configure the parameters. See Procedure 31-9 for more information.

14 Click on the Interface tab button. To configure interface-level (also known as neighbor) RIP parameters:

i Click on the Create button. The RIP Interface (Create) form opens.

ii Configure the parameters. See Procedure 31-10 for more information.

15 Click on the following tab buttons to view statistics and alarm information.

- Statistics
- Faults

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The RIP Site (Edit) form closes.

Procedure 31-9 To configure group-level RIP

Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the group-level RIP configuration.

Note 2 — The parameters that you configure for a RIP group take precedence over the parameters that are configured for the global-level RIP configuration.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to the RIP icon. The path is Routing→Router→Routing Instance→RIP.

3 Right-click on the RIP icon and choose Create Group. The RIP Site Group (Create) form opens with the General tab displayed.

4 Configure the Name parameter.

5 Perform steps 4 to 12 of Procedure 31-8.

6 Click on the OK button. The RIP Group (Create) form closes, and the 5620 SAM displays an icon for the new RIP group in the navigation tree below the RIP icon.

Procedure 31-10 To configure interface-level RIP

Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the interface-level RIP configuration.

Note 2 — The parameters that you configure for a RIP interface, also known as a RIP neighbor, take precedence over the parameters that are configured for the group- and global-level RIP configuration.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to a RIP group. The path is Routing→Router→Routing Instance→RIP→RIP Group.

3 Right-click on the RIP group icon and choose Create Interface. The RIP Interface (Create) form opens with the General tab displayed.

4 Perform steps 4 to 12 of Procedure 31-8.

5 Click on the OK button. The RIP Interface (Create) form closes, and the 5620 SAM displays an icon for the new RIP interface below the RIP group icon in the navigation tree.

31.17 LDP configuration procedures

An LDP instance in the 5620 SAM network navigation tree has the following child objects:

- Interfaces–The interfaces object contains the configured LDP interfaces for directly connected peers. The 7210 SAS-M does not support configuration of LDP interfaces.
- Targeted Peers–The targeted peers object contains the indirectly connected peers.

T-LDP is supported on the 7750 SR, 7710 SR, 7450 ESS, 7210 SAS-M, 7210 SAS-X, 7250 SAS-ES, 7705 SAR, and 7250 SAS-ESA. DU-LDP is supported only on the 7750 SR.

The following procedures describe how to configure LDP.

Procedure 31-11 To enable LDP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable LDP.

  i Click on the Protocols tab button.

  ii Select the LDP Enabled parameter.

5 Click on the OK button to save the changes. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an LDP icon appears under the routing instance in the navigation tree.

Procedure 31-12 To configure global-level LDP

1 Enable LDP on the router, as described in Procedure 31-11.

2 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

3 Navigate to the LDP instance icon. The path is Routing→Router→Routing Instance→LDP.

4 Right-click on the LDP icon and choose Properties. The LDP - Routing Instance (Edit) form appears, with the General tab displayed.

5 Configure the Administrative State parameter.

6 Click on the Common tab button.

7 Configure the parameters:

- Targeted Sessions Allowed
- Prefer Tunnel-in-Tunnel
- Tunnel Down Damp Time (seconds)
- Enable Implicit Null Label
- Enforce Graceful Restart
- Multi Path Make Before Break Time (seconds)
- Neighbor Liveness Time (seconds)
- Maximum Recovery Time (seconds)
- Forward State Holding Time (seconds)
- Reconnect Time (seconds)
- Shortcut Local TTL Propagate
- Shortcut Transit TTL Propagate
- Enable Fast Re-route

Configure the Targeted Sessions Allowed parameter to true to configure the router for T-LDP. Targeted sessions are LDP sessions that distribute labels between indirectly connected peers.

The Neighbor Liveness Time (seconds) and Maximum Recovery Time (seconds) parameters are configurable when the Enforce Graceful Restart parameter is enabled.

8 Click on the Interface Properties tab button.

9 Configure the parameters:

- Address Type
  - Choose system to have the system IP address set up LDP sessions.
  - Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.
- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

By default, these parameter values are inherited by all LDP interfaces.

10 Click on the Targeted Peer Properties tab button.

i Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

  By default, these parameter values are inherited by all LDP targeted peers.

ii Click on the Route Import Policy tab.

iii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

iv Click on the Route Export Policy tab.

v Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

11 Click on the Ecmp OAM tab button. The General tab displayed. See Procedure 31-16 for more information about configuring ECMP for LDP interfaces.

12 Click on the Interfaces tab button. A list of interfaces you can view or configure opens. See Procedure 31-13 for more information about configuring LDP interfaces.

13 Click on the Peers tab button. A list of peers you can view or configure opens. See Procedure 31-16 for more information about creating peers.

14 Click on the Targeted Peers tab button. A list of targeted peers you can view or configure opens. See Procedure 31-14 for more information about creating and configuring targeted peers.

15 Click on the Import Policies tab button.

16 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

17 Click on the Export Policies tab button.

18 Configure the parameters on the General tab:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

19 Click on the Tunnel Table tab button.

20 Configure the parameters on the Tunnel Table tab:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The tunnel table policies are used to allow LDP-capable PE devices to offer services to PE routers in areas or domains where BGP-labeled routes are not supported. They are used to determine which routes are advertised to LDP. Only policy entries supporting the LDP protocol are considered; all other policies are ignored. See also Procedure 31-5 for information on enabling the advertisement of LDP prefixes to BGP peers.

21 Click on the Sessions tab button. A list of LDP sessions opens, showing information of the active LDP communication sessions between interfaces and targeted peers between the routers running LDP.

22 Click on the Static Prefix FECs tab button.

i Click on the Create button. The StaticFec (Create) form opens.

ii Configure the parameters:

- IP Prefix
- Probe Interval (Minutes)
- Advertised Label
- Next Hop Type
- Next Hop
- Swap Label

Next Hop Address and Swap Label parameters appear when IP Address is selected for the Next Hop Address value.

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The static FEC form closes and the static FEC entry appears in the list.

23 Click on the Aggregate Prefix Match tab button.

24 Configure the parameters:

- Aggregate Prefix Match Enabled
- Administrative State

When the Aggregate Prefix Match Enabled parameter is enabled, the LDP installs a prefix binding in the LDP FIB by performing a longest match against an aggregate prefix in the routing table, as opposed to requiring an exact match of the prefix. The LDP prefix binding continues to be advertised on a per individual /32 prefix basis.

The Administrative State parameter can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

25 Configure the following parameters in the Prefix Exclude Policies block:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The Prefix Exclude Policies can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

When routing policy statements are specified in the Prefix Exclude Policies block, any prefixes defined in the routing policies are excluded from the aggregate prefix matching procedure. In this case, when LDP receives a FEC-label binding for this prefix, it performs an exact match of a specific FEC element prefix, as opposed to a longest match of one or more LDP FEC element prefixes.

26 Click on the Accounting tab button.

27 Click on the Create button. The AccountingFecPrefix (Create) form opens.

28 Configure the FEC Prefix parameter.

29 Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - AccountingFecPrefix form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedLdpLspEgressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

30 Click on the following tab buttons to view LDP statistics and alarm information.

- Statistics
- Faults

31 Click on the OK button. The LDP (Edit) form closes.

Procedure 31-13 To configure an LDP interface

Note — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP instance. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP instance and choose Create Interface. The LDP Interface configuration form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - LDP Interface form opens.

5 Configure the filter criteria. A list of the available interfaces appears.

6 Select an interface in the list and click on the OK button.

7 Configure the parameters:

- Description
- Administrative State

8 Click on the Protocol Properties tab button.

9 Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
- Address Type
    - Choose system to have the system IP address set up LDP sessions.
    - Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.

  By default, these parameter values are inherited by all LDP interfaces.
- Local LSR ID
- Enable BFD Tracking
- Multicast Forwarding

10 Click on the OK button. The LPD Interface (Create) form closes, and an icon for the new LDP interface appears in the navigation tree list of interfaces below the LDP icon.

11 Click on the OK button. An icon for the new LDP interface appears in the navigation tree below the LDP icon.

12 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 31-14 To configure an LDP targeted peer

Note 1 — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

Note 2 — The parameters that you configure for a targeted peer take precedence over the parameters that are configured for the global-level LDP configuration.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Create Targeted Peer. The TargetedPeer (Create) configuration form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- Description
- Administrative State

5 Click on the Protocol Properties tab button.

i Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
  By default, these parameter values are inherited from the global-level LDP instance.
- Tunneling Enabled
- BFD Enabled

ii Configure the Local LSR ID Name parameter by clicking on its associated Select button. The Select Local LSR ID window opens.

iii Select the desired Local LSR ID from the list and then click OK. The Select Local LSR ID window closes and the name of the Local LSR ID you chose appears in the Name field.

6 Click on the LSPs tab button. View, add, or configure associated LSPs, as required.

Refer to Chapter 32 for information on creating and configuring LSPs.

7 Click on the OK button. The TargetedPeer (Create) form closes, and an icon for the new LDP targeted peer appears in the navigation tree list of targeted peers below the LDP icon.

8 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 31-15 To configure an LDP peer

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP (Edit) form opens.

4 Click on the Peers tab button.

5 Click on the Create button. The Peer (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Peer Address
- Minimum TTL Value
- DoD Label Distribution
- Path MTU Discovery Enabled

7 Assign a TCP key chain to the LDP peer, if required.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select LDP Peer Keychain - Peer form opens with a list of local key chains displayed.

iii Select a key chain in the list and click on the OK button. The Select LDP Peer Keychain - Peer form closes. The 5620 SAM assigns the key chain to the LDP peer.

8 Select the Authentication tab button.

9 Configure the parameters:

- Type
- Key

10 Click on the Import Policies tab button.

The FEC prefix Import Policy provides a mean of controlling which FEC prefixes received from other LDP and T-LDP peers should be re-distributed to this LDP peer. If no policy name is specified, the NE will import all FEC prefixes it learns from other LDP and T-LDP peers to this LDP peer.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

12 Click on the Export Policies tab button.

The FEC prefix Export Policy provides a mean of controlling which FEC prefixes from this peer should be re-distributed to all other LDP and T-LDP peers. If no policy name is specified, the NE will export all FEC prefixes it learns from this LDP peer to all other LDP and T-LDP peers.

13 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The new peer appears in the list.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The LDP (Edit) form closes.

Procedure 31-16 To configure ECMP for LDP routing

Note — 5620 SAM supports LDP ECMP when LDP routing is configured on the 7750 SR, 7450 ESS, and 7710 SR.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP Routing Instance (Edit) form opens.

4 Click on the ECMP OAM tab button.

5 Perform one of the following steps:

   a If the Tree Trace parameter is not configured, go to step 6.

   b If the Tree Trace parameter is configured, go to step 7.

6 Select Configured from the Tree Trace drop-down menu. The LDP Routing Instance (Edit) form re-opens with all parameters displayed.

7 Configure the tree discovery configuration parameters:

- Tree Trace
- Administrative State
- Discovery Interval (Minutes)
- Discovery Timeout (Seconds)
- Retry Count
- Maximum Paths
- Forwarding Class
- Profile
- Maximum TTL
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Probe Interval (Minutes)
- Probe Timeout (Minutes)
- Retry Count

8 Click on the Discovered FECs tab. A list of discovered FECs appears.

9 Select a FEC from the list and click on the Properties button. An Autodiscovered FEC (Edit) form opens with the General tab displayed.

10 Perform one of the following:

   a Click on the More Actions button and choose Create LDP Tree Trace to configure and execute an LSP trace test; see chapter 38 for information about configuring this test.

   b Click on the More Actions button and choose Create LSP Ping to configure and execute a LSP ping test; see chapter 38 for information about configuring this test.

   c Click on the More Actions button and choose Create LSP Trace to configure and execute a LDP tree trace; see chapter 38 for information about configuring this test.

11 Click on the Discovered ECMP tab. A list of ECMP paths associated with the FEC appears.

12 Select an ECMP path from the list.

13 Click on the Properties button. An Autodiscovered Path (Edit) form opens.

14 Click on the More Actions button and choose Create LSP. To configure and execute an LSP trace test; see chapter 38.

15 Click on the More Actions button and choose Create LSP Ping. To configure and execute an LSP ping test; see chapter 38.

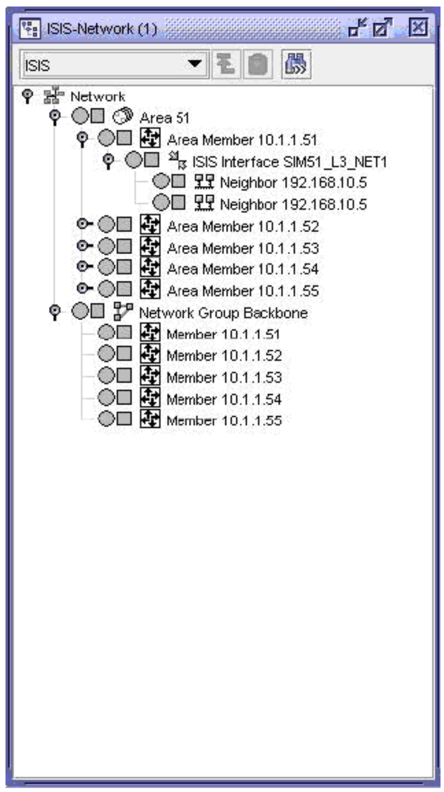
16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Autodiscovered FEC (Edit) form closes.

31.18 IS-IS configuration procedures

Configuration planning is essential to organize devices in level 1, level 2 and level 1 and 2 areas. IS-IS provides defaults for basic protocol operability. Use the 5620 SAM to configure the IS-IS parameters. Figure 31-7 shows the IS-IS view in the navigation tree

Figure 31-7 IS-IS view



The IS-IS information that is displayed includes:

- backbone area and backbone-area devices
- a list of areas and the participating routers in each area
- a list of devices and associated interfaces that shows the IP address and the configured level (1, 2, or 1 and 2) of each interface
- the IS-IS adjacencies for each interface

The following procedures describe how to configure IS-IS.

Procedure 31-17 To enable IS-IS on a routing instance

1. From the 5620 SAM GUI, choose Routing from the navigation tree view selector.
2. Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.
3. Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.
4. Enable the IS-IS protocol.
   i. Click on the Protocols tab.
   ii. Select the IS-IS Enabled parameter.
5. Click on the OK button. A dialog box appears.
6. Click on the Yes button. IS-IS is listed in the configuration form of configured protocols.
7. Click on the OK button. A dialog box appears.
8. Click on the Yes button. The Routing Instance (Edit) form closes, and an ISIS icon appears in the navigation tree below the routing instance.

Procedure 31-18 To configure IS-IS on a routing instance

Router-wide IS-IS parameter values can differ from the interface IS-IS parameter values that are configured in Procedure 31-20. Interface capabilities are compared to the outer-wide capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that are set up between routers to exchange IS-IS routing information.

1. Enable the IS-IS protocol on a router, as described in Procedure 31-17.
2. Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.
3. Right-click on the ISIS icon and choose Properties. The IS-IS Interface (Edit) form opens with the General tab displayed.
4. Configure the parameters:
   - Administrative State
   - Level Capability

   A level 1 adjacency can be established when there is at least one area address shared by this router and a neighboring router. A level 2 adjacency is established when another router is configured as a level 2 or a level 1 and 2 router with interfaces configured as level 2 or level 1 and 2. A level 1 and 2 adjacency is created when the neighboring router is also configured as a level 1 and 2 router and the routers have at least one area address in common.
5. Click on the Behavior tab button.

6 Configure the parameters:

- Reference Bandwidth
- Traffic Engineering
- Unicast Import
- Multicast Import
- Hello Authentication
- CSNP Authentication
- PSNP Authentication
- Multi-Topology
- IPv6 Unicast Multi-Topology
- Enable LDP Synchronization
- LDP over RSVP Include
- Isis Default Route Tag
- Advertise Only Passive Interfaces
- RSVP Shortcut Enabled
- Advertise Tunnel Links Enabled
- Enable Loop-free Alternate
- Overload On Boot
- Overload On Boot Timeout (seconds)
- Overload
- Overload Timeout (seconds)
- LSP Lifetime (seconds)
- LSP Max Wait (seconds)
- LSP Initial Wait (seconds)
- LSP Second Wait (seconds)
- SPF Max Wait (seconds)
- SPF Initial Wait (milliseconds)
- SPF Second Wait (milliseconds)

7 Click on the Graceful Restart tab button.

8 Configure the parameters:

- Graceful Restart
- Helper Mode

9 Depending on the device type and configuration, the IP Versions tab is configurable. Click on the IP Versions tab button to specify the allowed IP versions for the IS-IS instance.

10 Configure the parameters:

- Enable IPv6
- IPv6 Routing TLV type
- Enable IPv4
- Strict Adjacency Check

11 Click on the Authentication tab button.

12 Configure the parameters:

- Enable Authentication
- Type
- Key

13 Click on the Level 1 tab button. The General tab is displayed.

14 Configure the parameters:

- Preference
- Preference
- Wide Metrics Only
- Hello Authentication
- CSNP Authentication
- PSNP Authentication

15 Click on the Authentication tab button to configure level 1 authentication.

16 Configure the parameters:

- Type
- Key

Configure the authentication parameters to specify the MD5 key or password to verify PDUs from neighboring routers on the interface.

17 Click on the Level 2 tab button.

18 Repeat steps 14 to 16.

19 Click on the Export Policies tab button.

20 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

You can specify up to five routing policies, in order of preference, to determine the routes that are exported from the routing table to IS-IS. When multiple policies are specified, the policies are evaluated in order, from one to five.

21 Click on the NET addresses tab button. Perform step 4 of Procedure 31-19.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The new NET address appears on the NET Addresses tab.

24 Click on the Route Summarizations tab button. IS-IS route summaries allow users to create aggregate IPv4 or IPv6 addresses that include multiple groups of IPv4 or IPv6 addresses for a specific IS-IS summary level. This can help reduce the size of the link state database and the routing table.

25 Click on the Create button. The Route Summarization (Create) form opens.

26 Configure the parameters:

- Network
- Mask
- Summary Level
- Summary Route Tag

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The new route summary appears on the form.

29 Click on the Interfaces tab button to add an IS-IS interface, if required.

- **i** Click on the Create button.
- **ii** Perform steps 4 to 17 of Procedure 31-20.
- **iii** Click on the OK button. A dialog box appears.
- **iv** Click on the OK button. The new interface appears on the form.

30 Click on the following tab buttons to view information.

- Adjacencies
  - An adjacency represents a connection between two IS-IS interfaces. The information listed for an adjacency includes the state of the adjacent interface, the interface ID, and the neighbor ID.
- SPF Logs
- Statistics
- Faults

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The IS-IS (Edit) form closes.

Procedure 31-19 To configure an IS-IS NET address

1 Enable the IS-IS protocol on a device, as described in Procedure 31-17.

2 Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.

3 Right-click on the ISIS icon and choose Add NET Address. The Area ID (Create) form opens.

4 Configure the NET address for IS-IS using the Area ID parameter. The NET address is exchanged in hello and LSP PDUs. Level 1 interfaces must have at least one area ID in common. Level 2 interfaces can have different area IDs. If all of the interfaces have different area IDs, they are considered level 2 interfaces only.

NET addresses are built from some non-configurable elements, including the device system ID, the network SAP, and the network entity title.

5 Click on the OK button. The Area ID (Create) form closes, and an icon for the new area appears in the navigation tree below the ISIS icon.

Procedure 31-20 To configure an IS-IS interface

Interface IS-IS parameters can differ from the global policies set in Procedure 31-18. Interface-level parameters specify the interface routing levels. Interface level capabilities are compared to the router-wide capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that can be created between devices to exchange IS-IS routing information.

1 Enable the IS-IS protocol on a router, as described in Procedure 31-17.

2 Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.

3 Right-click on the ISIS icon and choose Create Interface. The IS-IS Interface (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State
- Level Capability
- Type
- BFD Enabled
- IPv6 BFD Enabled

5 Click on the Select button to choose a Layer 3 interface. The Select Interface - IS-IS Interface form opens.

6 Configure the filter criteria. A list of the available interfaces appears.

7 Select an interface in the list and click on the OK button.

8 Click on the Behavior tab button.

9 Configure the parameters:

- CSNP Interval (seconds)
- LSP Pacing Interval (seconds)
- Retransmit Interval (seconds)
- Mesh Group Status

  To create a mesh group, set the Mesh Group Status parameter to Enabled and specify the same mesh group number for all interfaces. The mesh group parameters specify the assigned mesh group for the interface. Mesh groups limit the amount of flooding when a new or changed LSP is advertised in an area.
- Mesh Group
- Passive
- Route Tag

The TE Metric check box is a read-only field that indicates whether the TE Metric parameter is being configured in the interface for LSP path computation by CSPF.

10 Click on the Authentication tab button.

11 Configure the parameters:

- Type
- Key

You can enable authentication for any IS-IS PDUs sent by the interface. Configure the authentication parameters to specify the MD5 key or password to verify PDUs that are sent by neighboring routers on the interface.

12 Click on the Level 1 tab button.

13 Configure the parameters on the General tab:

- Hello Interval (seconds)
- Hello Multiplier
- Metric
- Passive
- Priority

14 Click on the Authentication tab button.

15 Configure the parameters:

- Type
- Key

16 Click on the Level 2 tab button.

17 Repeat steps 13 to 15.

18 Click on the following tab buttons to view information.

- Adjacencies
  - An adjacency represents a connection between two IS-IS interfaces. The information listed for an adjacency includes the state of the adjacent interface, the interface ID, and the neighbor ID.
- Statistics

19 Click on the OK button. The IS-IS Interface (Create) form closes, and the new interface appears in the navigation tree below the ISIS icon.

31.19 OSPF configuration procedures

The 5620 SAM supports the configuration of OSPFv2 and OSPFv3.

Note 1 — OSPFv3 configuration is supported on the 7750 SR (chassis modes C and D, and also chassis modes A and B with mixed mode enabled), 7710 SR, 7450 ESS (mixed mode), and 7705 SAR, Release 4.0 and later.

Note 2 — OSPFv2 configuration is supported on the 7705 SAR Release 2.0 and later.

Note 3 — The 7750 SR, 7450 ESS, 7710 SR, OS 9700E, and OS 9800E support multiple instances of OSPFv2 on the base routing instance.

Note 4 — The 7450 ESS in mixed mode, the 7710 SR, and the 7750 SR in chassis mode C or D support multiple OSPF instances in VPRN services.

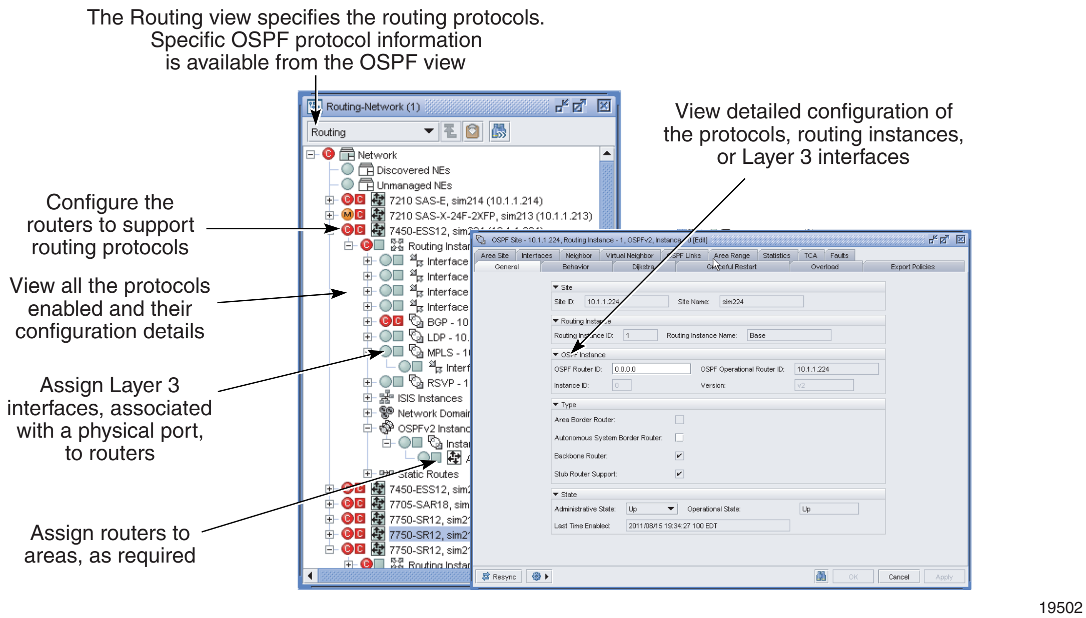
Note 5 — The 7210 SAS-M supports only one OSPF instance.

Configuration planning is essential to organize OSPF areas, interfaces, and virtual links. OSPF provides defaults for basic protocol operability. OSPF configuration requires, as a minimum, that:

- you create a single OSPF backbone area that contains the area border routers.
- for larger networks, you create several areas that contain the other routers.
- for smaller networks, you place all routers in the OSPF backbone area.

Use the 5620 SAM navigation tree to configure the OSPF parameters. Figure 31-8 shows the OSPF view in the navigation tree.

Figure 31-8 OSPF view



The OSPF parameters that are required for OSPF deployment are:

- Router ID — Each device that runs OSPF must be configured with a unique router ID. The router ID is used by the OSPF and BGP routing protocols in the routing table manager. When you configure a new router ID, protocols are not automatically restarted with the new router ID. You must shut down and restart the protocol to initialize the new router ID.
- An area — At least one OSPF area must be created. An interface must be assigned to each OSPF area. The types of OSPF areas include a backbone area, stub area, and NSSA.
- Layer 3 interfaces — A Layer 3 interface is the logical IP connection between a router and one of its attached networks. A physical interface is associated with the Layer 3 interface to provide the cabled connected to another device. A Layer 3 interface has state information from the underlying lower-level protocols and the routing protocol. A network interface has an associated IP address and mask that combine to create an IP prefix, unless the interface is in an unnumbered, point-to-point network.

The following procedures describe how to configure OSPF.

Procedure 31-21 To enable OSPF on a routing instance

1. Choose Routing from the navigation tree view selector from the 5620 SAM GUI.
2. Navigate to the routing instance icon by choosing Routing→Router→Routing Instance.
3. Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab button.

5 Select the OSPFv2 Enabled parameter to enable OSPFv2, if required.

6 Select the OSPFv3 Enabled parameter to enable OSPFv3, if required.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Routing Instance (Edit) form closes, and an icon for each newly enabled protocol appears under the routing instance in the navigation tree.

Procedure 31-22 To configure OSPF on a routing instance

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the OSPF area that you need to add a router by choosing one of the following:

   a 7750 SR, 7450 ESS, and 7710 SR, Network→Router→Routing Instance→OSPFv*N* Instances.

   b For all other devices, Routing→Router→Routing Instance→OSPFv*N*, where *N* is the OSPF version number; for example, 2 or 3

3 Perform one of the following, when OSPFv2 is required:

   a For the 7705 SAR, right-click on the appropriate OSPFv2 Instances icon and choose Properties. The OSPF Site, Routing instance, OSPFv2 instance (Edit) form appears. Go to step 5.

   b For the 7750 SR, 7450 ESS, or 7710 SR, right-click on the appropriate OSPFv2 Instances icon and choose Create OSPFv2 Instance. The OSPF (Create) form opens with the General tab displayed. Go to step 5.

4 For OSPFv3:

   i Right-click on the appropriate routing instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

   ii Click on the Protocols tab button and ensure the OSPFv3 Enabled parameter is configured to create the OSPFv3 routing instance. Click on the appropriate OSPFv3 Instances icon.

   iii Select the appropriate Instance icon below the OSPFv3 Instances icon, and select Properties. The OSPF Routing Instance OSPFv3 (Edit) form opens.

5 Configure the parameters:

- OSPF Router ID
- Instance ID
- Autonomous System Border Router
- Domain ID
- Administrative State

6 Click on the Behavior tab button.

7 Configure the parameters:

- Traffic Engineering Support
- Interface Base Reference Cost (kbps)
- Overload Stubs
- Unicast Import
- Multicast Import
- Enable LDP Synchronization
- Ignore DN Bit
- Suppress DN Bit
- RFC1583 Compatible
- LDP over RSVP Include
- Advertise Tunnel Links Enabled
- Exit Overflow Interval
- External LSA Limit
- Preference
- Preference

The Traffic Engineering Support, RFC1583 Compatible, LDP over RSVP Include, Multicast Import, and Unicast Import parameters are configurable for OSPFv2 only.

The Unicast Import and Multicast Import parameters are not configurable for OSPF in VPRN.

8 Click on the Dijkstra tab button.

9 Configure the following parameters:

For SPF:

- SPF Max Wait (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)

For LSA:

- LSA Generate Max Wait (milliseconds)
- LSA Arrival Wait (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)

10 Depending on the OSPF version, the Graceful Restart tab is configurable. Configure graceful restart, if required.

i Click on the Graceful Restart tab button.

ii Configure the parameters:

- Graceful Restart
- Helper Mode

The Helper Mode parameter is configurable when the Graceful Restart parameter is set to true.

11 Depending on the OSPF version, the Overload tab is configurable. Configure overload, if required.

i Click on the Overload tab button.

ii Configure the parameters:

- Overload Enabled
- Boot Overload Enabled
- Overload Interval (seconds)
- Boot Overload Interval (seconds)

The Overload Interval (seconds) parameter is configurable when the Overload Enabled parameter is selected.

The Boot Overload Interval (seconds) parameter is configurable when the Boot Overload Enabled parameter is enabled.

12 If the OSPF version is OSPFv2, the OSPF Super-Backbone tab is configurable. Configure the OSPF super-backbone, if required.

i Click on the OSPF Super-Backbone tab button.

ii Configure the parameters:

Note — These parameters apply only to VPRN instances of OSPF.

- VPN Domain Type
- VPN Domain ID (hex)
- VPN Tag
- Super-Backbone

13 Click on the Export Policies tab button to specify the export routing policies that determine the routes that are advertised to peers.

14 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

15 Click on the Area Site tab button to add a routing instance for the router to an OSPF area, if required. Otherwise, go to step 17.

- **i** Click on the Create button. The AreaSite (Create) form opens.
- **ii** Configure the parameters:
  - Area ID
  - Type
  - Blackhole Range
- **iii** Click on the OK button. The AreaSite (Create) form closes, and the OSPF (Edit) form reappears.

16 Perform steps 4 to 13 of Procedure 31-25.

17 Click on the following tab buttons to view OSPF configuration information:

- Interfaces
- Neighbor
- Virtual Neighbor
- Virtual Link (configurable only in a backbone area)
- Area Range
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for OSPF in VPRN.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to close the OSPF Site (Edit) form.

Procedure 31-23 To create an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Right-click on the Network icon and choose Create Area. The Area (Create) form opens.

3 Configure the parameters:

- Version
- Area ID
- Name
- Type
- Description

4 Click on the Apply button. Additional configurable tab buttons appear.

5 Click on the Area Site tab button.

6 Click on the Create button to add a routing instance to the area. The Area Site (Create) form opens.

7 Click on the Select button to choose a routing instance. The Select OSPF Instance - Area Site form opens.

8 Select an OSPF instance and click on the OK button. The Select OSPF Instance form closes, and the OSPF instance appears in the Routing Instance panel.

9 Configure the parameters:

- Type
- Blackhole Range

Configure the area as a blackhole range to avoid routing loops.

The Type parameter is not configurable for a backbone-area routing instance.

10 Click on the Apply button. Additional configurable tab buttons appear, and an icon for the new area appears in the navigation tree.

11 Depending on the Type parameter value, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

The Default Cost parameter is configurable only when the Type parameter value from step 9 is Stub (No Type 5 External) or Totally Stub (No Summaries).

i Click on the Stub/NSSA tab button.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route

The Redistribute External Routes and Originate Default Route parameters are configurable only when the Type parameter value from step 9 is NSSA (No Type 5 External) or NSSA (No Summaries).

12 If the area is a backbone area that requires links to remote areas that do not advertise OSPF topology, configure a virtual link.

i Click on the Virtual Link tab button.

ii Perform steps 4 to 8 of Procedure 31-27.

iii Click on the OK button. The new virtual link entry appears in the list.

13 Create an area range, if required.

i Click on the Area Range tab button.

ii Click on the Create button. The Area Range (Create) form opens.

iii Perform steps 4 and 5 of Procedure 31-26.

iv Click on the OK button. The new area range entry appears in the list.

14 Click on the OK button. The Area Site (Create) form closes, and a dialog box appears.

15 Click on the Yes button to confirm the action.

Procedure 31-24 To add a router to an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Navigate to the OSPF area to which you want to add a router. The path is Routing→Area.

3 Right-click on the area icon and choose Add OSPF Instance. The Area Site (Create) form opens.

4 Configure the parameters:

- Type
- Blackhole Range

Configure the area as a blackhole range to avoid routing loops.

5 Click on the Select button below the Routing Instance panel to choose a routing instance. The Select OSPF Instance - Area Site form opens.

6 Select a routing instance and click on the OK button. The routing instance appears in the Routing Instance panel.

7 Depending on the Type parameter value from step 4, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

i Click on the Stub/NSSA tab button.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route

The Default Cost parameter is configurable only when the Type parameter value from step 4 is Stub (No Type 5 External) or Totally Stub (No Summaries).

The Redistribute External Routes and Originate Default Route parameters are configurable only when the Type parameter value from step 4 is NSSA (No Type 5 External) or NSSA (No Summaries).

8 Click on the OK button. The Area Site (Create) form closes, and an icon for the router appears in the navigation tree under the Area icon.

Procedure 31-25 To add a Layer 3 interface to an OSPF router

Perform this procedure to allow an OSPF-enabled router to participate in area discovery and share routing information with other area members.

Note — This action assigns an existing Layer 3 interface to the router in the OSPF area rather than creating a new Layer 3 interface.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon to display the area routers.

3 Right-click on a router instance icon and choose Create Interface. The OSPF Interface (Create) configuration form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State
- Configured MTU (bytes)

5 Click on the Select button beside the Interface Name parameter to choose an interface. The Select Interface - OSPF Interface form opens.

6 Configure the filter criteria. A list of available Layer 3 interfaces appears.

7 Choose a Layer 3 interface and click on the OK button. The Select Interface - OSPF Interface form closes, and the interface entry appears in the Interface panel.

8 Click on the Protocol Properties tab button.

9 Configure the parameters:

- Type
- Priority
- Metric
- Advertise Subnet
- BFD Enabled
- Passive
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

The Advertise Subnet parameter is configurable for OSPFv2 only.

The TE Metric check box is a read-only field that indicates whether the TE Metric parameter is being configured in the interface for LSP path computation by CSPF.

10 Perform one of the following steps to configure authentication for the interface, if required. Otherwise, go to step 13.

a Click on the Authentication tab button, and go to step 11.

b For OSPFv3 interfaces, click on the IPsec Static SA tab button, and go to step 12.

11 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

12 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

13 Click on the OK button to close the OSPF Interface (Create) form. The 5620 SAM displays an icon for the new OSPF interface in the navigation tree below the area router.

Procedure 31-26 To create an OSPF area range

An area range summarizes a range of IP addresses in an LSA to minimize the number of flooded advertisements in the LSA.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon in the navigation tree to display the area routers.

3 Right-click on a router instance icon and choose Create Area Range. The Area Range (Create) form opens.

4 Configure the parameters:

- Network
- Prefix Length
- Link State DB Type
- Effect

5 Click on the OK button. The Area Range (Create) form closes, and an icon for the new area range appears in the navigation tree below the OSPF area.

Procedure 31-27 To create a virtual link

Perform this procedure to create a link between the backbone OSPF area and a remote OSPF area that does not advertise the OSPF topology.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on the backbone area icon in the navigation tree to display the area routers. The backbone area ID is 0.0.0.0.

3 Right-click on a backbone-area router instance icon and choose Create Virtual Link. The Virtual Link (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Virtual Neighbor Router (Site) ID
- Transit Area
- Administrative State

5 Click on the Protocol Properties tab button.

6 Configure the parameters:

- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

7 Perform one of the following steps to configure authentication for the virtual link, if required. Otherwise, go to step 10.

a Click on the Authentication tab button, and go to step 8.

b For OSPFv3 interfaces, click on the IPsec Static SA tab button, and go to step 9.

8 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

v Go to step 10.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

v Go to step 10.

9 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VirtualLink (Create) form closes, and the 5620 SAM displays an icon for the new virtual link in the navigation tree.

31.20 RSVP configuration procedures

The following procedures describe how to configure RSVP.

Procedure 31-28 To configure RSVP on a routing instance

1 Navigate to an RSVP icon. The path is Routing→Router→Routing Instance→RSVP.

2 Right-click on the RSVP icon and choose Properties. The RSVP form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- Keep Multiplier
- Refresh Time
- Message Pacing
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Max Burst
- Period (milliseconds)
- Rapid Retransmit Time (hundred-milliseconds)
- Rapid Retry Limit

4 If you are going to configure Diff-Serv TE, then MPLS must be shutdown first. Otherwise, go to step 16.

5 Configure the parameters:

Note 1 — Enabling a Diff Serv Model only takes effect if you have already enabled traffic engineering at one or both of the following routing protocol levels:

- IS-IS, as described in Procedure 31-18
- OSPF, as described in Procedure 31-22

A dialog box appears if IS-IS and/or OSPF TE is not enabled, but you can save your configuration if IS-IS and/or OSPF TE is not enabled.

Note 2 — The Class Type BW Percent parameters are configured globally and the parameters are applied to all RSVP interfaces in the system. After the parameters are configured, the parameters can only be changed after you shut down the MPLS protocol. The total bandwidth specified for the eight classes should not exceed 100%.

- Diff Serv Model
- TE Threshold Update Enabled
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent
- Update On CAC Failure Enabled
- Update Timer (seconds)

6 Configure the Include Node in RRO parameter.

7 Click on the TE Classes tab.

8 Select one of the TE classes in the table and click on the Properties button. The TE Class (Create) form opens.

Note — The TE Class Definition is used to map all TE Classes (up to a maximum of 8) to Class Type and LSP setup priority. There is no default TE Class after Diff-Serv is enabled. You must explicitly define each TE Class. If Diff-Serv is disabled, the default CT (CT0) and eight pre-emption priorities are used internally.

9 Configure the parameters:

- Priority
- TE Class Type

10 Click on the ForwardingClassMaps tab.

11 Click on the Create button. The Forwarding Class Map (Create) form opens.

12 Configure the parameters:

- FC Name
- TE Class Type

13 Repeat steps 8 to 12 for the remaining TE classes, as required.

14 Click on the TE Thresholds tab.

15 Configure the parameters:

- Up Threshold (%) (1 through 16)
- Down Threshold (%) (1 through 16)

You can also click the Reset TE Up/Down Thresholds to Default buttons to set either the Up or Down Thresholds to their default values, respectively.

16 Click on the following tab buttons to view information.

- Interfaces
- Sessions
- Neighbors
- Statistics
- Faults

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The RSVP form closes.

Procedure 31-29 To configure an RSVP interface

1 Navigate to an RSVP interface icon. The path is Routing→Router→Routing Instance→RSVP→Interfaces→Interface.

2 Right-click on the RSVP interface and choose Properties. The RSVP Interface (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Administrative State

4 Click on the Protocol Properties tab button.

5 Configure the parameters:

- Enable Refresh Reduction
- Enable Reliable Delivery
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Hello Interval (milliseconds)
- Subscription Ratio
- BFD Enabled
- Inherit SAM Class Type BW
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent

The Class Type BW Percent parameters can only be configured if the Inherit SAM Class Type BW parameter is disabled. If you enter values at the RSVP interface level, they override the global values configured in Procedure 31-28 for the node RSVP routing instance.

6 Click on the Authentication tab button.

7 Configure the Key parameter.

8 Click on the TE Thresholds tab.

9 Configure the parameters:

- Inherit TE Up Thresholds
- Inherit TE Down Thresholds
- Up Threshold (%) (1 through 16)
- Down Threshold (%) (1 through 16)

You can only configure the Up Threshold (%) and Down Threshold (%) parameters if the Inherit TE Up Thresholds and Inherit TE Down Thresholds parameters are disabled, respectively.

10 Click on the following tab buttons to view information.

- Neighbors
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The RSVP Interface (Edit) form closes.

31.21 L2TP configuration procedures

The 5620 SAM supports the configuration and management of L2TP sites, tunnel group profiles, and tunnel profiles.

A typical L2TP configuration is applied to two NEs; one NE performs the LAC role and the other NE performs the LNS role. An NE can perform both LAC and LNS roles. At least one ISA-LNS group must be configured for the LNS NE. See section 18.5 for information about ISA-LNS groups. See Procedure 18-7 for information about creating and configuring an ISA-LNS group member.

Note 1 — To enable L2TP, the NE must be in chassis mode B or higher.

Note 2 — The 7750 SR, Release 7.0, does not support L2TP in chassis mode B.

Note 3 — The 5620 SAM supports L2TP configuration and management on a Release 7.0 or 8.0 7750 SR, or a 7450 ESS in mixed mode, for LAC only.

Note 4 — L2TP can also be enabled on a VPRN site. See chapter 74 for more information.

The following procedures describe how to configure L2TP.

Procedure 31-30 To configure L2TP on a routing instance

Note 1 — Only a Release 8.0 or later 7750 SR-7 or 7750 SR-12 can function as an LNS.

Note 2 — L2TP functionality is supported only by Ethernet MDAs. An IOM 2 or IOM 3 is required to configure an L2TP access interface, and an IOM 3 is required for an L2TP network interface. An IOM3-XP is required for configuration of a broadband ISA MDA.

1 Navigate to an L2TP icon. The path is Routing→Router→Routing Instance→L2TP.

2 Right-click on the L2TP icon and choose Properties. The L2TP Site (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- Session Limit
- Receive Window Size
- Peer Address Change Policy
- Excluded AVPs
- Calling Number Format

4 Click on the Tunnel Group Profiles tab button.

i Click on the Create button. The L2TP Tunnel Group Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Group Name
- Description
- Administrative State
- Local IP Address
- Local Name
- LNS Group ID
- Password
- Challenge
- AVP Hiding
- Session Limit
- Session Assign Method
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)

Note 1 — You must configure the LNS Group ID parameter for the tunnel group profile or tunnel profile of the site acting as the LNS.

Note 2 — On the LAC NE, each L2TP tunnel must have the local IP address set to the system interface IP address. This restriction applies only to the 7750 SR, Release 7.0.

Note 3 — To generate operational L2TP tunnels, a start operation must be performed on the L2TP tunnel on the LAC NE. You can also perform a start operation from a tunnel profile on the LNS.

5 Click on the PPP tab button.

Note — You only configure PPP for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

6 Configure the Authentication Protocol parameter.

7 Click on the Select button in the Authentication Policy panel. The Select Authentication Policy (PPPGroupProfile) form opens.

8 Select an authentication policy from the list and click on the OK button. The Select Authentication Policy form closes and the L2TP Tunnel Group Profile (Create) form displays the new PPP authentication policy.

9 If you did not select an authentication policy in step 8, click on the Select button in the User Database panel. The Select User Database (PPPGroupProfile) form opens.

10 Select a user database from the list and click on the OK button. The Select User Database form closes and the L2TP Tunnel Group Profile (Create) form displays the user database.

11 Click on the Select button in the Default Service ID panel. The Select Default Service ID (PPPGroupProfile) form opens.

12 Select a default service ID from the list and click on the OK button. The Select Default Service ID form closes and the L2TP Tunnel Group Profile (Create) form displays the default service ID.

13 Click on the Select button in the Default Group Interface panel. The Select Default Group Interface (PPPGroupProfile) form opens.

14 Select a default group interface from the list and click on the OK button. The Select Default Group Interface form closes and the L2TP Tunnel Group Profile (Create) form displays the default group interface.

15 Configure the parameters:

- Proxy LCP
- Proxy Authentication
- MTU (bytes)
- Keep-Alive Interval (seconds)
- Keep-Alive Multiplier
- IPCP Subnet Negotiation

16 Click on the Tunnel Profiles tab button.

i Click on the Create button. The L2TP Tunnel Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Tunnel Name
- Description
- Administrative State
- Local IP Address
- Local Name
- Peer IP Address
- Remote Name
- LNS Group ID
- Password
- Auto Established
- Preference
- Challenge
- AVP Hiding
- Session Limit
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)

Note — When you configure parameters with the same name in a tunnel group profile and a tunnel profile, a non-default value in the tunnel group profile overrides the value specified for the L2TP site. Also, a non-default value in a tunnel profile overrides the value defined in the associated tunnel group profile and L2TP site.

17 Click on the PPP tab button.

Note — You only configure PPP for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

18 Repeat steps 6 to 15 to configure PPP for an LNS L2TP tunnel profile.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The L2TP Tunnel Profile (Create) form closes.

21 Click on the following tab buttons to view information.

- Tunnel Instance Endpoints
- Peers
- Statistics
- Faults

Procedure 31-31 To view L2TP tunnels and tunnel endpoints

1 Choose Manage→ISA Functions→ISA-L2TP from the 5620 SAM main menu. The Manage ISA-L2TP form opens.

2 Choose L2TP tunnel (L2TP) from the object drop-down list.

3 Click on the Search button. A list of L2TP tunnels is displayed.

4 Select an entry in the list and click on the Properties button. The L2TP Tunnel - Endpoint A - Endpoint B form opens with the General tab displayed.

5 View the information for Tunnel Endpoint A and Tunnel Endpoint B.

6 Click on the L2TP Tunnel Endpoints tab button. The two L2TP tunnel endpoints are displayed.

7 Select an entry in the list and click on the Properties button. The L2TP Tunnel Endpoint (View) form opens.

8 View the information. You can also click on the Properties button to view additional information for the following:

- Site ID
- Tunnel Instance Endpoint
- Tunnel Profile
- Tunnel Group Profile
- Peer

9 Close the L2TP Tunnel Endpoint (View) form.

10 Close the L2TP Tunnel - Endpoint A - Endpoint B form.

31.22 PIM configuration procedures

The following procedures describe how to configure PIM.

Procedure 31-32 To enable PIM on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable PIM:

i Click on the Multicast tab button.

ii Select the PIM Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and a PIM icon appears in the navigation tree below the routing instance.

Procedure 31-33 To configure PIM on a routing instance

1. From the 5620 SAM GUI, choose Routing from the navigation tree view selector.
2. Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.
3. Right-click on the PIM icon and choose Properties. The PIM (Edit) form opens with the General tab displayed.
4. Configure the Administrative State parameter in the States panel.
5. In the PIM General Configurations panel, configure the following parameters:
   - Apply To
   - Non DR Attract Traffic
6. In the ECMP Balancing panel, configure the following parameters:
   - ECMP Balancing Enabled
   - Hold Time (minutes)
   - ECMP Hashing Enabled
7. In the Lag Usage panel, configure the Lag Usage Optimization parameter.
8. Click on the RP Behavior tab button.
9. If you are configuring for IPv4 then click on the IPv4 sub-tab and go to step 10. Otherwise click on the IPv6 sub-tab and go to step 15.
10. Configure the IPv4 Administrative State parameter in the States panel.
11. Configure the following parameters in the PIM General Configurations panel:
    - IPv4 RPF Lookup Sequence
12. Configure the following parameters in the Candidate Bootstrap Router panel:
    - CBSR Address
    - CBSR Priority
    - CBSR Hash Mask Length
    - CBSR Admin State
13. Configure the following parameters in the Candidate Rendezvous Point panel:
    - Administrative State
    - C-RP Address
    - C-RP Priority
    - C-RP Hold Time (seconds)
14. Go to step 20.
15. Configure the IPv6 Administrative State parameter in the States panel.
16. Configure the IPv6 RPF Lookup Sequence parameter in the PIM General Configurations panel.

17 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length
- CBSR Admin State

18 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

19 Configure the following parameters in the Embedded-RP panel:

- Enable Embedded-RP
- Embedded-RP Administrative State

20 Click on the Candidate-RP Groups tab.

21 Click on the Create button to add a new entry, if required. The C-RP Group Prefix (Create) form opens.

22 Configure the parameters:

- Group IP Address
- Mask

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The C-RP Group Prefix (Create) form closes and the new Candidate-RP entry appears in the table.

25 Click on the Embedded-RP Groups tab button.

Note — The Embedded-RP Groups tab is only selectable if you enabled the Enable Embedded-RP parameter in step 19.

26 Click on the Create button to add a new entry, if required. The E-RP Group Range (Create) form opens.

27 Configure the parameters:

- Group IP Address
- Prefix

28 Click on the OK button. The E-RP Group Range (Create) form closes and the new Embedded-RP entry appears in the table.

29 Click on the Group To RP tab button.

30 In the Static RP tab, click on the Create button to add a new entry, if required. The Static RP (Create) form opens.

31 Configure the parameters:

- Static RP IP Address
- RP Override

32 Click on the Static Group-To-RP tab button.

33 Click on the Create button to add a new entry, if required. The Static Group To RP (Create) form opens.

34 Configure the parameters:

- Static Group IP Address
- Static Group Mask

35 Click on the OK button. A dialog box appears.

36 Click on the OK button. The new Static Group-To-RP entry appears on the form.

37 Click on the OK button. A dialog box appears.

38 Click on the OK button. The new Static RP entry appears on the form.

39 If you are performing this procedure to create a PIM site on a VPRN routing instance (referenced from Procedure 74-5), the MVPN tab button appears. Click on the MVPN tab button. Otherwise, go to step 49.

40 Configure the parameters on the General sub-tab:

- Auto-Discovery
- MCast Signaling
- Inclusive Tunnel Type
- US Multicast Hop Selection
- Inter-Site Shared

Note — You must set the Inclusive Tunnel Type parameter to PIM, RSVP, or MLDP if you are creating an inclusive tunnel in step 45.

41 Click on the UMH PE Backup sub-tab to configure primary and standby UMH addresses, if required.

42 Click on the Create button. The MVPN UMH PE Backup (Create) form opens.

43 Configure the parameters:

- UMH Primary PE Address
- UMH Standby PE Address

44 Click on the OK button. The MVPN UMH PE Backup (Create) form closes and the new entry appears in the list.

45 Click on the MVPN Inclusive Tunnel tab button.

Note — Only one sub-tab will be active under the MVPN Inclusive Tunnel tab, depending on the selection you made for the Inclusive Tunnel Type parameter in step 40.

Perform one of the following:

a Create a PIM inclusive tunnel, if required.

i Configure the parameters on the PIM tab button:

- Provider Tunnel Inclusive PIM Mode
- Group Address

  The Group Address parameter is only configurable if the Provider Tunnel Inclusive PIM Mode parameter is set to ASM or SSM.

ii Go to step 46.

b Create an RSVP inclusive tunnel, if required.

i Configure the P2MP Administrative State parameter on the RSVP tab button. Until you have selected an MVPN LSP template, you cannot set the P2MP Administrative State parameter to Up. To create an MVPN LSP template, see Procedure 32-23.

ii Click on the Select button. The Select MVPN Lsp Template form opens.

iii Choose an MVPN LSP template from the list and click on the OK button. The MVPN LSP template is displayed.

iv Configure the parameters:

- Tunnel Root Enable BFD
- Tunnel Root BFD Transmit Interval
- Tunnel Root BFD Multiplier
- Tunnel Leaf Enable BFD

v Go to step 46.

c Create an MLDP inclusive tunnel, if required.

i Configure the P2MP Administrative State parameter on the MLDP tab button.

ii Go to step 46.

46 Click on the MVPN Selective Tunnel tab button. The Data MVPN Threshold tab is displayed.

47 Configure the parameters:

- PIM SSM Prefix
- PIM SSM Prefix Length
- PIM Group Address Mode
- Delay Interval (seconds)
- Pack Data Join TLV
- Auto-Discovery
- Enable ASM Data MDT

The Delay Interval (seconds) parameter can only be configured if the Include Data parameter is enabled.

48 Perform one of the following:

a Click on the Search button in the Data MVPN Threshold tab.

i Select a Data MVPN Threshold entry from the displayed list.

ii Click on the Apply button.

iii Go to step 49.

b Click on the Create button in the Data MVPN Threshold tab. The Data MVPN Threshold (Create) form is displayed.

i Configure the parameters:

- Group IP Address
- Group Prefix Length
- Threshold (kbps)

ii Click on the OK button. The Data MVPN Threshold (Create) form closes and the new entry is displayed in the list.

iii Select the new Data MVPN Threshold entry.

iv Click on the Apply button.

49 Perform one of the following, if required:

Note — A Data Multicast Tunnel (MT) can be thought of as a connector between a set of PE routers forming a multicast domain. From the perspective of a VPN-specific PIM instance, a multicast tunnel is a single multi-access interface. The Data MT Interface can only be created or selected when the PIM address is configured as other than null (0.0.0.0).

a Click on the Search button in the Data MT Interface tab.

- **i** Choose a Data MT Interface entry from the list.
- **ii** Click on the Apply button.
- **iii** Go to step 50.

b Click on the Create button in the Data MT Interface tab. The Data MT Interface (Create) form is displayed.

- **i** Configure the parameters:
    - Administrative State
    - Hello Interval (seconds)
    - Hello Multiplier
    - Improved assert
    - Three Way Hello
    - Tracking Support
- **ii** Click on the OK button. The Data MT Interface (Create) form closes and the new entry is displayed in the list.
- **iii** Select the new Data MT Interface entry.
- **iv** Click on the Apply button.

50 Click on the Import Policies tab button.

51 Click on the BootStrap Import Policies tab button.

52 Configure the parameters to filter bootstrap messages and to control the flow of bootstrap messages to the routing instance.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

53 Click on the Join/Prune Import Policies tab button.

54 Configure the parameters to filter join/prune messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

55 Click on the Register Import Policies tab button.

56 Configure the parameters to filter PIM register messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

57 Click on the Export Policies tab button.

58 Click on the BootStrap Export Policies tab button.

59 Configure the parameters to filter PIM-related export messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

60 Depending on the device version, the Anycast RP tab is configurable. Click on the Anycast RP tab button to configure Anycast RP, if required.

Note — You can use the PIM configuration form to add peers to an anycast RP. The complete configuration of anycast RP for PIM requires additional supporting components, such as the configuration of loopback interfaces and static RPs. Due to the complex configuration dependencies, Alcatel-Lucent recommends that you use the Virtual Anycast manager. The Virtual Anycast manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities. See Procedure 31-34 for more information about using the Virtual Anycast manager.

61 Click on the General tab button.

62 Configure the RP IP Address parameter.

63 Click on the Anycast Peer tab button.

64 Click on the Create button to create a new entry, if required. The Anycast Peer (Create) form opens.

65 Configure the Peer IP Address parameter.

66 Click on the OK button. A dialog box appears.

67 Click on the OK button. The new anycast peer entry appears on the form.

68 Click on the OK button. A dialog box appears.

69 Click on the OK button. The new anycast RP entry appears on the form.

70 Click on the SSM Groups tab button.

71 Click on the Create button to create a new entry, if required.

72 Configure the parameters:

- SSM Group IP Address
- SSM Group Mask

  These parameters are applicable to both IPv4 and IPv6.

73 Click on the OK button. A dialog box appears.

74 Click on the OK button. The new SSM group entry appears on the form.

75 Click on the Interfaces tab button to create an interface, if required.

i Click on the Create button to add a new entry.

ii Perform steps 4 to 10 of Procedure 31-35.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new interface entry appears on the form.

76 Click on the SPT Switch Threshold tab button to configure SPT switchover, if required.

77 Click on the Create button to create a new entry, if required. The Spt Switch Over Threshold (Create) form opens.

78 Configure the parameters:

- Group IP Address
- Group Prefix Length
- Infinity For Threshold
- Threshold (kbps)

79 Click on the OK button. A dialog box appears.

80 Click on the OK button. The new SPT switch threshold entry appears on the form.

81 Click on the following tab buttons to view and edit information.

- Groups
- Neighbor
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for PIM in VPRN.

82 Click on the OK button. A dialog box appears.

83 Click on the Yes button. The PIM (Edit) form closes.

Procedure 31-34 To configure Anycast PIM on a router

This procedure describes how to use the Virtual Anycast Manager to configure anycast PIM on a router. The Virtual Anycast Manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities.

Note — The 5620 SAM does not automatically delete the supporting requirements for the protocol when you delete an anycast RP member.

You can also manually add peers to an anycast RP by navigating to the Anycast RP tab of the PIM configuration form. Ensure that PIM is enabled on the router. See Procedure 31-33 for more information.

The 5620 SAM raises an alarm when VRFs from different VPRNs are added to a single anycast RP set. You can only mismatch VRFs using methods that are not associated with the Virtual Anycast Manager; for example, by using the CLI or the PIM configuration form.

1 Choose Manage→Networking→Virtual Anycast RP from the 5620 SAM main menu. The Manage Virtual Anycast RP form opens.

2 Click on the Create button. The Virtual Anycast RP form opens with the General tab displayed.

3 Configure the parameters:

- Anycast RP Type
- Anycast RP Address
- Name
- Description
- Auto Created Interface Name

4 If the Anycast RP Type parameter value is VPRN, choose a VPRN service for the anycast RP.

i Click on the Select button. The Select Service form opens.

ii Select a VPRN service in the list and click on the OK button. The Select Service form closes, and the service is displayed in the Service panel.

5 Click on the Apply button. The Status panel appears. The Status panel is used in step 9 of this procedure to identify configuration problems.

6 Click on the Components tab button.

7 Add virtual Anycast RP members to the PIM configuration.

i Right-click on the Virtual Anycast RP Members icon and choose Add Anycast RP Member. The Enter Interface Name form opens.

ii Enter the interface name for the loopback interface. The Auto Created Interface Name parameter value appears, if configured.

iii Click on the OK button. The Enter Interface Name form closes, and the Select Local Address form opens.

iv Configure the filter criteria.

v Select the local IP address that is used to communicate with the other RP members in the virtual anycast set and click on the OK button. The new local address entry appears on the Components tab under the Virtual Anycast RP Members icon. The new local address entry also appears under the Static RP icon.

Note — The local address is typically the system address.

The 5620 SAM automatically performs the following virtual anycast RP required configuration tasks.

- It creates a PIM-enabled loopback interface, if not present, with the RP address.
- It adds a local address to the anycast RP peer set.
- It updates the peer sets that participate in the anycast RP so that all peer sets contain the same members.
- It enables PIM on the interface that contains the local IP address.
- It creates a static RP that uses the anycast RP address. Groups must be manually created using the Components tab.

vi Repeat steps 7 i to v for each member in the virtual anycast RP.

8 Add a static group-to-RP mapping for the anycast configuration.

i Right-click on a member in the Static RP list and choose Create Static RP. The Static RP (Create) form opens.

ii Configure the parameters:

- Static Group IP Address
- Static Group Mask

iii Click on the OK button. The Static Group To RP (Create) form closes.

iv Repeat steps 8 i to iii for each static group-to-RP mapping that you want to add to the virtual anycast RP configuration. Each member needs a static RP and at least one static group-to-RP mapping. The mappings typically use the same configuration values for each member in the group.

9 Verify the status of the anycast RP for PIM configuration.

i Click on the General tab button. The Status panel displays the status of the anycast RP configuration. The 5620 SAM updates the status when you add a member to or delete a member from the virtual anycast RP. You can also use the Update Status button to manually update the Status panel.

Table 31-2 lists the status check boxes that identify potential configuration problems.

Table 31-2 Anycast RP status fields

Check box	Description
Missing Group Range(s) Configurations	At least one anycast RP member does not have a group range for the anycast RP address.
Inconsistent Peer Sets	Peer sets of all the anycast RP members are not equal.
PIM not enabled on loopback interface(s)	PIM is not enabled on all loopback interfaces that are configured in the virtual anycast RP.
Only one peer configured	Only one peer is configured for anycast RP. The configuration requires two or more peers for correct functionality.
Loopback interface(s) not properly configured	At least one anycast RP member does not have a loopback interface configured with the anycast RP address.
Missing Static RP configuration(s)	A member of the virtual anycast RP does not have a static RP. Each member requires a static RP.

ii Click on the OK button. The Manage Virtual Anycast RP form reappears, and the new virtual anycast RP entry appears on the form.

iii Close the Manage Virtual Anycast RP form.

Procedure 31-35 To create a PIM interface

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.

3 Right-click on the PIM icon and choose Create Interface. The PIM Interface (Create) form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - PIM Interface form opens.

5 Configure the filter criteria.

6 Select an interface in the list and click on the OK button. The Select Interface - PIM Interface form closes, and the interface name appears in the Interface panel.

7 Configure the parameters:

- Description
- Administrative State
- BFD Enabled
- IPv6 BFD Enabled

8 Click on the Behavior tab button.

9 Click on the General sub-tab.

10 Configure the parameters:

- Hello Interval (seconds)
- Hello Multiplier
- Tracking Support
- Multicast Senders
- BSM Check Router Alert
- Improved assert
- Assert Period
- Max Groups
- Three Way Hello
- Sticky DR
- DR Priority
- Sticky DR Priority

The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

11 Click on the Neighbor tab button, if configurable, to view and edit information. The Neighbor tab is configurable only when a neighbor PIM interface exists.

12 Click on either the IPv4 or IPv6 sub-tab, as required.

13 Configure either the IPv4 Administrative State or IPv6 Administrative State parameter in the States panel, as required.

14 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

ii Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - PIM Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

iv Click on the Levels tab.

v Click on the Create button. The PIM Interface Multicast CAC level form opens.

vi Configure the parameters:

- Level ID
- Bandwidth (kbps)

vii Click on the LAG Port Down tab.

viii Click on the Create button. The PIM Interface Multicast CAC LAG Port Down form opens.

ix Configure the parameters:

- Number of Ports Down
- Level

15 Click on the OK button. The PIM Interface (Create) form closes, and an icon for the new PIM interface appears in the navigation tree below the PIM icon.

31.23 IGMP configuration procedures

The 5620 SAM supports IGMP configuration for core router functionality and IP services.

The following procedures describe how to configure IGMP.

Procedure 31-36 To enable IGMP on a router

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) configuration form opens.

4 Enable IGMP.

i Click on the Multicast tab button.

ii Select the IGMP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an IGMP icon appears in the navigation tree below the routing instance icon.

Procedure 31-37 To configure IGMP on a router

1. From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2. Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3. Right-click on the IGMP icon and choose Properties. The IGMP Site (Edit) form opens with the General tab displayed.

4. Configure the parameters:

   - Administrative State
   - Query Interval (seconds)
   - Last Member Query Interval (seconds)
   - Query Response Interval (seconds)
   - Robust Count

5. Click on the SSM Translation tab button to configure SSM, if required.

   i. Click on the Create button to create a new entry. The SSM Translation (Create) form opens.

   ii. Configure the parameters:

      - Start Mcast Address
      - End Mcast Address
      - Configured Source

   iii. Click on the OK button. A dialog box appears.

   iv. Click on the OK button. The new SSM entry appears on the form.

6. Click on the Interfaces tab button to add an interface, if required.

   i. Click on the Create button.

   ii. Perform steps 4 to 15 of Procedure 31-39.

   iii. Click on the OK button. The new interface entry appears on the form.

7. Click on the Group Interfaces tab button to view IES group interfaces added to IGMP, if required.

8. Click on the LDP Tunnel Interfaces tab button to create an LDP tunnel interface entry, if required.

   i. Click on the Create button. The LDP IGMP Tunnel Interface (Create) form opens with the General tab button displayed.

   ii. Click on the Select button next to the P2MP ID parameter. The Select - LDP IGMP Tunnel Interface form opens.

   iii. Select an LDP tunnel interface and click on the OK button. The LDP IGMP Tunnel Interface form reappears with the information displayed.

   iv. Click on the Static Group/Source tab button to create a static multicast entry, if required.

v Click on the Create button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the LDP IGMP Tunnel Interface (Create) form.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The LDP IGMP Tunnel Interface (Create) form closes.

9 Click on the RSVP Tunnel Interfaces tab button to create an RSVP tunnel interface entry, if required.

i Click on the Create button. The RSVP IGMP Tunnel Interface (Create) form opens with the General tab button displayed.

ii Click on the Select button next to the Lsp Name parameter. The Select - RSVP IGMP Tunnel Interface form opens.

iii Select an RSVP IGMP tunnel interface and click on the OK button. The Select - RSVP IGMP Tunnel Interface form closes and the RSVP IGMP Tunnel Interface (Create) form reappears with the information displayed.

iv Click on the Static Group/Source tab button to create a static multicast entry, if required.

v Click on the Create button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the form.

ix Click on the OK button. A dialog box appears. The RSVP IGMP Tunnel Interface (Create) form closes and the new tunnel entry is displayed.

x Click on the OK button. The RSVP IGMP Tunnel Interface (Create) form closes.

10 Click on the following tab buttons to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Routing Instance (Edit) form closes.

Procedure 31-38 To configure IGMP on an OmniSwitch

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→ Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Properties. The IGMP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Querying
- Spoofing
- Proxying
- Querier Forwarding
- Zapping
- Max Group Action
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)

Note — When the Administrative State parameter is Up, IP multicast switching is enabled on the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes.

Note — IGMP parameters can also be configured for each VLAN site. The VLAN site IGMP configuration overrides the routing instance IGMP settings. You can only configure VLAN site IGMP parameters after the VLAN is created. See Procedure 69-15 for information about configuring IGMP on an OmniSwitch.

Procedure 31-39 To create an IGMP interface

Note — IGMP IPv6 interfaces are supported on the 7750 SR in chassis mode A or B with mixed mode enabled, and on the 7750 SR in chassis mode C or D.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Create Interface. The IGMP Interface (Create) form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - IGMP Interface form opens.

5 Configure the filter criteria.

6 Select an interface in the list and click on the OK button. The Select Interface - IGMP Interface form closes, and the interface name appears in the Interface panel.

7 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

8 Click on the Behavior tab button.

9 Configure the Import Policy parameter.

10 Configure the Disable Router Alert Check parameter, if required.

11 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

ii Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - IGMP Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

12 Click on the SSM Translation tab button, if required.

i Click on the Create button.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source
- Start Mcast Address Type
- End Mcast Address Type
- Configured Source Type

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM translation entry appears on the form.

13 Click on the Static Group/Source tab button to create a static multicast entry, if required.

i Click on the Create button.

ii Configure the parameters:

- Static Multicast Group
- Static Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new static multicast entry appears on the form.

14 Click on the following tab buttons to view and edit information.

- Multicast Group
- Multicast Group/Source

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The IGMP Interface (Create) form closes, and an icon for the new interface appears in the navigation tree below the IGMP icon.

Procedure 31-40 To turn up or shut down an IGMP interface

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the interface icon and choose Properties. The IGMP Site (Edit) form opens.

4 Click on the Interfaces tab button.

5 Turn up or shut down the IGMP interface.

a Click on the Turn Up button to activate the interface. A dialog box appears.

b Click on the Shut Down button to deactivate the interface. A dialog box appears.

6 Click on the Yes button to confirm the action and close the dialog box.

7 Close the IGMP Site (Edit) form.

Procedure 31-41 To view IGMP multicast reporting statistics for an IGMP site

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Networking→Routing Instances from the 5620 SAM main menu. The Manage Routing Instances form opens.

2 Choose IGMP Site (IGMP) from the Select Object Type drop-down menu.

3 Click on the Search button to display the IGMP sites.

4 Choose a site from the list and click on the Properties button. The IGMP Site form opens with the General tab displayed.

5 Click on the More Actions button and choose Show IGMP Multicast Reporting Statistics. The IGMP IGMP Stats Show IGMP Multicast Reporting Statistics form opens.

6 Configure the IP address, if required.

7 Click on the OK button. The contents of the IGMP multicast report are displayed.

8 Close the IGMP IGMP Stats Show IGMP Multicast Reporting Statistics form.

Procedure 31-42 To view IGMP source statistics

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Search button to display a list of services.

3 Choose a service from the list and click on the Properties button. The Service (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button to display a list of sites.

5 Choose a site from the list and click on the Properties button. The Site (Edit) form opens with the General tab displayed.

6 Click on the Multicast tab button.

7 Click on the Group Interfaces tab button to display a list of group interfaces.

8 Choose a group interface from the list and click on the Properties button. The IGMP Group Interface (Edit) form opens with the General tab displayed.

9 Click on the Group Interface SAP tab button.

10 Choose a group interface SAP from the list and click on the Properties button. The Group Interface SAP (Edit) form opens with the General tab displayed.

11 Click on the Group tab button.

12 Click on the Search button to display a list of groups.

13 Choose a group from the list and click on the Properties button. The Group Interface SAP Group (View) form opens with the General tab displayed.

14 Click on the Source tab button.

15 Click on the Search button to diplay a list of sources.

16 Close the Group Interface SAP Group (View) form.

17 Click on the Statistics tab button.

18 Click on the Collect button to collect additional statistics.

19 Choose a statistics record from the list and click on the Properties button. The Statistics Record - Group Interfact SAP Stats form opens.

20 Review the statistics and close the Statistics Record - Group Interface SAP Stats form.

21 Close the IGMP Group Interface SAP (Edit) form.

22 Close the IGMP Group Interface (Edit) form.

23 Close the Site (Edit) form.

24 Close the Service (Edit) form.

25 Close the Manage Services form.

31.24 MSDP configuration procedures

The MSDP command hierarchy consists of three levels:

- global level
- peer level and group level
- group peer level

MSDP parameters are initially applied at the global level. These parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

The following procedures describe how to configure MSDP.

Procedure 31-43 To enable MSDP on a router

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable MSDP by performing the following steps.

   i Click on the Multicast tab button.

   ii Select the MSDP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Confirm the action. The Routing Instance (Edit) form closes, and an MSDP icon appears in the navigation tree below the routing instance icon.

Procedure 31-44 To configure global-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- SA Limit
- Data Encapsulation
- Local IP Address
- RPF Lookup Sequence
- SA Cache Lifetime (seconds)
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Group tab button to add a group, if required. See Procedure 31-45 for more information about how to configure a group-level MSDP.

6 Click on the Peer tab button to add a peer, if required. See Procedure 31-46 for more information about how to configure a peer-level MSDP.

7 Click on the Source tab button to add a source, if required. See Procedure 31-47 for more information about how to configure an MSDP source.

8 Click on the Import Policies tab button.

9 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

10 Click on the Export Policies tab button.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. A router performs no validation to ensure the policies match.

12 Click on the following tab buttons to view information.

- Data Source Active
- Statistics
- Faults

13 Click on the OK button. A dialog box appears.

14 Confirm the action. The MSDP (Edit) form closes.

Procedure 31-45 To configure group-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Group. The MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Mode
- SA Limit
- Local IP Address
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Peer tab button to add a peer, if required.

6 Click on the Create button. The MSDP Peer Group (Create) form opens.

7 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

8 Configure the import and export policies for the MSDP peer by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

9 Click on the Authentication tab button.

10 Configure the parameters:

- Type
- Key

11 Click on the OK button. The MSDP Peer Group (Create) form closes and a dialog box appears.

12 Confirm the action. The peer is listed on the MSDP Peer Group (Create) form.

13 Configure the import and export policies for the MSDP group by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

14 Click on the OK button. The MSDP Peer Group (Create) form closes, and an MSDP Peer Group icon appears in the navigation tree below the MSDP Routing Instance icon.

Procedure 31-46 To configure peer-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Peer. The MSDP Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab button.

7 Configure the parameters.

- Type
- Key

8 Click on the OK button. The MSDP Peer (Create) form closes, and an MSDP Peer icon appears in the navigation tree below the MSDP Routing instance icon.

Procedure 31-47 To configure an MSDP source

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Click on the Source tab button.

5 Click on the Create button. The MSDP Source (Create) form opens.

6 Configure the parameters:

- IP Prefix
- Mask
- SA Limit

7 Click on the OK button. The MSDP Source (Create) form closes and a dialog box appears.

8 Confirm the action. The source is listed on the MSDP (Edit) form.

9 Click on the OK button. A dialog box appears.

10 Confirm the action. The MSDP (Edit) form closes.

Procedure 31-48 To configure group-peer-level MSDP

Note — The parameters that you configure for a MSDP peer take precedence over the parameters that are configured for the MSDP peer group.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to a peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The MSDP Group Peer, MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 30. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab button.

7 Configure the parameters:

- Type
- Key

8 Click on the OK button. The MSDP Group Peer, MSDP Peer Group (Create) form closes, and an MSDP Group Peer icon appears in the Navigation Tree below the MSDP Peer Group icon.

Procedure 31-49 To enable or disable MSDP peering

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Perform one of the following:

a Enable or disable MSDP peering in a peer group.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

ii Right-click on an MSDP Peer Group icon.

b Enable or disable MSDP peering in a group peer.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group→MSDP Group Peer.

ii Right-click on an MSDP Group Peer icon.

3 Choose one of the following menu items:

a Turn Up to activate

b Shut Down to deactivate

A dialog box appears.

4 Click on the Yes button. The state information beside the appropriate MSDP icon changes accordingly.

31.25 MLD configuration procedures

MLD is supported on a chassis mode C or D, and on the 7750 SR in chassis mode A or B with mixed mode enabled.

The following procedures describe how to configure MLD.

Procedure 31-50 To enable MLD on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Right-click on the Routing Instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab and enable the MLD Enabled check box.

5 Click on the OK button. The Routing Instance (Edit) form closes, and an MLD icon appears in the navigation tree below the routing instance.

Procedure 31-51 To configure MLD on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MLD icon by choosing Network→Router→Routing Instance→MLD.

3 Right-click on the MLD icon and choose Properties. The MLD, Routing Instance (Edit) form opens with the General tab displayed.

4 Configure the optional parameters:

- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count

5 Click on the Apply button to save the changes.

6 Click on the SSM Translation tab button, and click on the Add icon. The SSM Translation, Routing Instance window opens.

7 Configure the mandatory parameters:

- Start Multicast Address
- End Multicast Address
- Configured Source

8 Click on the Apply button to save the changes.

If you wish to create an MLD interface from this window:

a Click on the Interface tab button and click on the Add icon. Go to step 4 of Procedure 31-52.

b Click on the OK button. The MLD, Routing Instance (Edit) form closes.

Procedure 31-52 To create an MLD interface on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MLD icon by choosing Network→Router→Routing Instance→MLD.

3 Right-click on the MLD icon and choose Create Interface. The MLD Interface, Routing Instance (Create) form opens with the General tab displayed.

4 Configure the optional parameter Description.

5 Click on the Select button. The Select Interface - MLD Interface - Routing Instance window opens.

6 Select an existing network interlace that has IPv6 enabled and click the OK button to save the entry. The Select Interface - MLD Interface - Routing Instance window closes and the MLD interface name appears in the navigation tree below the MLD icon.

7 Click on the Behavior tab button and configure the optional parameters:

- Disable Router Alert Check
- Maximum Number of Groups
- Query Interval (seconds)
- Maximum Response Time between Group Messages (seconds)
- Maximum Response Time For MLDv2 (seconds)

8 Click on the Apply button to save the changes.

9 Click on the Import Policy tab button.

10 Click on the Select icon to select an optional routing policy, or configure the optional parameter Import Policy.

11 Click on the Apply button to save the change.

12 Click on the Static/Group Source tab button and click on the Add icon. The MLD Group Source Static, null (Create) window opens.

13 Configure the mandatory Group Address parameter and the optional Group Source Address parameter.

14 Click on the Apply button to save the changes.

15 Click on the SSM Translation tab button and click on the Add icon. The MLD Interface Source Specific Multicast, null (Create) window opens.

16 Configure the mandatory parameters:

- Start Multicast Address
- End Multicast Address

17 Configure the optional parameter Group Source Address.

18 Click on the Apply button to save the changes.

19 Click on the OK button. The MLD Interface, Routing Instance (Create) form closes.

31.26 Bridging configuration procedures

The following procedures describe how to configure bridging.

Procedure 31-53 To configure bridging on a 7250 SAS or Telco device

This procedure applies to 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Click on an icon that represents a 7250 SAS or Telco device. The Bridge Instance icon appears.

3 Right-click on the Bridge Instance icon and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Click on the IGMP Snooping tab button.

5 Configure the parameters:

- IGMP Snooping
- Query Source IP Zero

You must set the IGMP Snooping parameter to Enabled before you can configure the Query Source IP Zero parameter. IGMP snooping is required in a BTV VLAN and when MVR is used in a ring group to which the device belongs.

6 Click on the TLS tab button to configure parameters associated with 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices in TLS VLAN ring groups.

7 Configure the parameters:

- TLS Admin Status
- Ethertype
- Jumbo Frame

The Jumbo Frame parameter is configurable only for Telco devices.

8 Click on the MVR tab button to configure parameters associated with 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices in BTV ring groups.

9 Configure the parameters:

- MVR Admin Status
- Mode
- Query Time (seconds)

The Mode parameter is configurable only for Telco devices.

10 Click on the Multicast Groups tab button to view the list of multicast group IP addresses for the specified VLAN.

11 Click on the QoS MAC Static tab button to configure static MAC QoS parameters for a port on the bridge.

Note — The QoS MAC Static tab button is not available for 7250 SAS and 7250 SAS-ES NEs, Release 2.0 or newer and the 7250 SAS-ESA.

i Click on the Create button. The QoS MAC Static Entry form opens.

ii Configure the parameters:

- Name
- Description
- MAC Address
- VLAN ID
- Priority

iii Click on the Select button to choose a physical port on the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device as an interface. The Select Interface form opens.

iv Select a port in the list and click on the OK button. The Select Interface form closes, and the port identifier appears in the Interface panel.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new static MAC QoS entry appears on the form.

12 Click on the QoS MAC Secure tab button to configure secure MAC QoS parameters for the bridge.

Note — The QoS MAC Secure tab button is not available for 7250 SAS and 7250 SAS-ES NEs, Release 2.0 or newer or the 7250 SAS-ESA.

i Click on the Create button. The QoS MAC Secure Entry form opens.

ii Configure the parameters:

- Name
- Description
- MAC Address
- VLAN ID
- Priority

iii Click on the Select button to choose a physical port on the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device as an interface. The Select Interface form opens.

iv Select a port in the list and click on the OK button. The Select Interface form closes, and the port identifier appears in the Interface panel.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new secure MAC QoS entry appears on the form.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The Bridge (Edit) form closes.

Procedure 31-54 To configure bridging on an OmniSwitch

Perform this procedure to configure OmniSwitch bridging, STP, and LPS parameters.

Caution — Changing bridge parameter values may affect the spanning tree calculations and trigger a topology change in the network.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- STP Mode
- Path Cost

Configure the Auto VLAN Containment parameter if you the chose the flat STP mode.

5 Configure LPS, if required.

i Click on the Learned Port Security tab button. The Learned Port Security General tab is displayed.

ii Configure the parameters:

- Learning Time Window (minutes)
- Status

Note 1 — The Status parameter does not appear on the form and the Restart Timer option is dimmed until you enter a non-zero value for the Learning Time Window (minutes) parameter.

Note 2 — Click on the More Actions button and choose Restart Timer to restart the MAC source learning timer if you need to restart dynamic MAC address learning on a port.

iii Click on the Ports tab button.

iv Click on the Create button to select ports on which you want to enable learned port security. The Select Port - Bridge form opens.

v Choose one or more ports and click on the OK button. The Select Port - Bridge form closes and the selected ports appear in the Ports form.

vi Click on the Apply button to enable learned port security on the selected ports. A dialog box appears.

vii Click on the Yes button.

viii If you need to apply the same LPS properties to multiple ports but do not need to configure static MAC addresses on the ports, go to step 5xxiv.

Note — Static MAC addresses can only be added to LPS-enabled ports individually.

ix Choose a port and click on the Properties button. The Learned Port Security (Edit) form opens.

x Click on the Properties button. The Physical Port (Edit) form opens on the General tab.

xi Click on the LPS Learned MAC Entries tab button.

xii Click on the Create button to add static MAC entries. The MAC Entries (Create) form opens.

Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses.

xiii Click on the Select button. The Select VLAN Site - MAC Entries form opens.

xiv Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

xv Choose a VLAN from the list.

xvi Click on the OK button. The Select VLAN Site - MAC Entries form closes.

xvii Configure the MAC Address parameter.

xviii Click on the Apply button to save the configuration.

xix Repeat steps 5xvii to 5xviii if you need to add another static MAC address to the port.

xx Click on the OK button. A dialog box appears.

xxi Click on the Yes button to close the dialog box.

xxii Click on the OK button to close the Physical Port (Edit) form. A dialog box appears.

xxiii Click on the Yes button. Go to step 5xxv.

xxiv Choose multiple ports and click on the Properties button. The Learned Port Security (Edit) form opens.

xxv Configure the parameters:

- Violation
- Administrative State
- Low MAC Range
- High MAC Range
- Max. MAC Addresses to Learn
- Max. Filtered MACs to Learn
- Trap Threshold

xxvi Click on the OK button to save the configuration and close the Learned Port Security (Edit) form.

xxvii If you need to stop the aging out of dynamic MAC addresses on the LPS port, convert the dynamic MAC addresses to static MAC addresses. Choose the port and click on the More Actions button and choose Convert to Static.

Note — If traffic containing MAC addresses outside of the allowable MAC address range attempts to access an LPS port, the switch either restricts access to the port for that traffic or shuts the port down to all traffic. When this happens, the port is in an operationally violated state and an alarm is raised.

See Procedure 31-55 for information about how to release a violated LPS port.

6 Perform one of the following actions:

a Configure the STP Flat Mode.

b Configure the STP 1x1 Mode; go to step 25.

7 Click on the Spanning Tree tab button. The STP Flat Mode CIST General tab is displayed.

8 Configure the parameters:

Caution — Changing the Protocol parameter to MSTP resets the flat bridge priority and path.

- Protocol
- Priority
- Forwarding Delay (seconds)
- Hello Time (seconds)
- Max Age (seconds)
- TX Hold Count
- Instance BPDU Switching

9 Click on the Port tab button.

10 Choose one or more ports from the list.

11 Click on the Properties button. The CIST Instance Ports (Edit) form opens.

12 Configure the parameters:

- Priority
- Path Cost
- Mode
- Connection Type
- Admin Edge
- Auto Edge
- Restricted Role
- Restricted TCN

13 Click on the OK button. The CIST Instance Ports (Edit) form closes.

14 Click on the MSTI tab button if you need to configure MSTI, otherwise go to step 34.

Note — In order to configure MSTI, the Protocol parameter must be set to MSTP.

15 Click on the Create button. The MST Instance (Create) form opens.

16 Configure the parameters:

- Instance Index
- Priority
- Instance Name
- Auto VLAN Containment

17 Click on the VLAN tab button.

18 Click on the Create button to assign a VLAN to the MSTI. The Select VLAN Sites - MST Instance form opens.

19 Choose one or more VLANs from the list and click on the OK button. The VLANs appear on the MST Instance VLAN form.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button.

22 Click on the MST Region tab button.

23 Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

24 Go to step 34.

25 Click on the Spanning Tree tab button.

Caution — Changing the STP 1x1 Mode configuration may affect the STP calculations for this instance of the VLAN and trigger a topology change in the network.

26 Click on the STP 1x1 Mode tab button.

27 Choose a 1x1 instance from the list and click on the Properties button. The VLAN STP Instance (Edit) form opens with the General tab displayed.

28 Configure the parameters:

- Protocol
- Forwarding Delay (seconds)
- Max Age (seconds)
- Instance BPDU Switching
- Priority
- Hello Time (seconds)
- TX Hold Count

29 Click on the Port tab button.

30 Choose one or more ports from the list of ports that have been assigned to VLANs and click on the Properties button. The VLAN STP Instance Ports (Edit) form opens.

31 Configure the parameters:

- Priority
- Mode
- Auto Edge
- Restricted Role
- Path Cost
- Connection Type
- Auto Edge
- Restricted TCN

32 Click on the OK button. The VLAN STP Instance Ports (Edit) form closes.

33 Click on the OK button. The VLAN STP Instance form closes.

34 Click on the TLS tab button.

35 Configure the TLS Mode parameter.

36 Click on the QoS tab button.

37 Configure the parameters:

- QoS Status
- Trust Ports
- Default Servicing Mode
- Default Bridged Disposition
- Default Routed Disposition
- Default IGMP Disposition

38 Click on the Apply button. A dialog box appears.

39 Click on the Yes button. The applied values for the Default Bridged Disposition, Default Routed Disposition, and Default IGMP Disposition parameters should be the same as the configured values.

40 Click on the IGMP Port Group Limit tab button.

41 Configure the filter criteria. A list of ports appears.

Note — Only ports that are active (administratively Up) appear in the list.

42 Choose one or more ports from the list and click on the Properties button.

43 The IGMP Port Group Limit (Edit) or IGMP Port Group Limit - (Multiple Instances) (Edit) form opens.

44 Configure the parameters:

- Port Max Group
- Port Action

45 Click on the OK button.

Note — Click on the Multicast VLAN Port tab button in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 69-19 for more information.

46 If you need to configure the IGMP port group limit parameters for an inactive (administratively Down) port, click on the Create button. Otherwise, go to step 57.

47 The Select Port form opens.

48 Configure the filter criteria. A list of ports appears.

49 Choose one or more ports from the list and click on the OK button. The Select Port form closes and the selected ports appear in the list of ports.

50 Choose an inactive port from the list and click on the Properties button.

51 Configure the parameters:

- Port Max Group
- Port Action

52 Repeat steps 50 and 51 for each inactive port that you need to configure.

53 Click on the Apply button. A dialog box appears.

54 Click on the Yes button to save your configuration.

Note 1 — The inactive ports do not appear in the list of ports. Only active ports are displayed in the list. You can view the configuration of the inactive ports using the OmniSwitch CLI.

Note 2 — Click on the Multicast VLAN Port tab button in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 69-19 for more information.

55 Click on the MVRP tab button to configure MVRP (if required).

56 Configure the parameters:

- VLAN Registration Protocol Type
- Status
- Transparent Switching Status
- Max VLAN

57 Click on the OK button. A dialog box appears.

58 Click on the Yes button. The Bridge (Edit) form closes.

Procedure 31-55 To release a violated OmniSwitch LPS port

Perform the following procedure to release a violated LPS port.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Click on the Learned Port Security tab button. The Learned Port Security General tab is displayed.

5 Click on the Port tab button.

6 Select one or more violated LPS ports. Violated LPS ports are highlighted in orange. When you select one or more violated ports the Release Violated Port option is enabled.

7 Click on the More Actions button and choose Release Violated Port to release the selected ports. Releasing a violated port restores the port to the same operational state it was in before the violation. When a violated port is released, all MAC addresses known to the port are flushed from the switch MAC address table.

8 Close the Bridge (Edit) form.

---

32 — MPLS

32.1 MPLS overview

The 5620 SAM supports the configuration and provisioning of MPLS paths and LSPs.

MPLS is a data-carrying mechanism that emulates some properties of a circuit-switched network over a packet-switched network. MPLS prepends a packet with an MPLS header that is comprised of labels in a stack. As an NE forwards a packet through an MPLS network, it examines the top label for routing instructions and pops it off the stack; the contents below the label stack are not examined. The label stack is not removed until it reaches the egress NE.

MPLS uses one or more IGPs, such as IS-IS, OSPF, or RIP, to forward packets. Regardless of the IGP chosen, the MPLS configuration is the same. An advantage of MPLS is that if more than one IGP is enabled, it continues to work when another protocol fails. See chapter 31 for more information on IS-IS, OSPF, and RIP.

MPLS can be used as the underlying transport mechanism for service tunnels. For MPLS to be used as such, an MPLS mesh and an LSP mesh must be created before the tunnel is created. Since LSPs and service tunnels are unidirectional, they must be created in both directions. See chapter 33 for more information about service tunnels.

When MPLS is enabled on a 5620 SAM-managed NE routing instance, the 5620 SAM displays an MPLS instance below the routing instance in the network view of the navigation tree. Using this view, you can perform various functions on the MPLS instance, for example, assign an L3 interface to an MPLS instance.

If a link, NE, or path fails, MPLS can determine a redundant path by using fast reroute. Fast reroute uses an alternative NE to complete the failed LSP. Fast reroute provides the following types of route protection.

- Many-to-one—one backup route is maintained for multiple protected LSPs on an NE.
- One-to-one—a separate backup route is maintained for each protected LSP on an NE algorithm.

You can list and view MPLS objects such as MPLS and RSVP instances and interfaces, static and dynamic LSPs, cross connections, and MPLS paths using the 5620 SAM Manage MPLS Objects form.

LSPs

An LSP is a path through an MPLS network that is set up based on criteria in a forwarding equivalency class, or FEC. A FEC is a set of characteristics that define how NEs in an MPLS network forward packets that are bound to an MPLS label. A FEC includes specifications such as the destination IP address and QoS parameters. A FEC is associated with a specific LSP, but an LSP may be used for multiple FECs.

An LSP begins at a PE device called an LER, which is the ingress NE that prepends a label to a packet based on a FEC and sends the packets to the next transit NE in the path. The transit NE swaps the packet label for a new one, and sends the packet to the next NE. The LER that acts as the egress PE NE removes the label and forwards the packet according to the header of the next layer, for example, IP.

LSPs are unidirectional; they enable the label switching of a packet through an MPLS network from one endpoint to another. Bidirectional communication through an MPLS network requires the configuration of an LSP in the opposite direction.

The types of LSPs are the following.

- Static LSPs specify a static path through an MPLS network. All transit NEs require manual configuration with LSP labels and require no signaling protocol, such as LDP or RSVP.
- Bypass-only LSPs are LSPs with manually configured bypass tunnels on Point-of-Local-Repair (PLR) nodes. Such LSPs are used exclusively for the purpose of bypass protection.
- Dynamic, or signaled LSPs, use a protocol such as LDP or RSVP. The signaling protocol allows an ingress NE to dynamically assign labels to an egress NE. You must configure the ingress NE, but not the transit NEs in an LSP. LDP LSPs are not explicitly defined. The downstream unsolicited (DU) method configures them automatically through the network.
- Point-to-Multipoint LSPs allow the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network.

You can apply a metric value to a dynamic LSP or a Point-to-Multipoint LSP that determines which LSP the 5620 SAM uses when multiple LSPs lead to the same destination. The metric value for a static route is set to 1 and cannot be configured.

You can list and view detailed information on LSPs, templates, cross connections, service tunnels, and detour and bypass information on the LSP (Edit) forms.

Dynamic LSPs

A dynamic LSP uses a signaling protocol such as LDP or RSVP-TE and an MPLS path between two NEs. You can then create an LSP between the two NEs and bind it to an MPLS path. An LSP-MPLS path binding is called an LSP path. You can configure the LSP path after the MPLS path and the LSP are bound.

Dynamic LSPs are categorized as follows:

- Explicit-path LSPs resemble static LSPs when all hops are strict; each hop in the LSP requires explicit configuration. MPLS uses RSVP-TE to set up an explicit-path LSP. Transit NE hops can be strict, and use a direct path between NEs, or loose, and include other NEs in the path between NEs.
- Constrained-path LSPs have dynamically assigned intermediate NE hops that rely on CSPF to find a path that satisfies the LSP constraints. CSPF is a routing algorithm that takes different LSP constraints, such as the available bandwidth and MPLS administrative groups, into account to balance the network load. When the CSPF path is found, RSVP uses the path to request the LSP setup. If Fast Reroute is enabled, the ingress NE signals the downstream NEs to set up a detour configuration for the LSP.

When an LSP is established, the reserved bandwidth is controlled by the bandwidth parameter at the primary path level, regardless of whether the LSP has auto-bandwidth enabled. When auto-bandwidth is enabled and a trigger occurs, the NE attempts to change the bandwidth of the LSP to a value between the minimum and maximum bandwidth, which are configurable at the LSP level. Automatic bandwidth allocation is supported on RSVP LSPs that have both CSPF and MBB enabled. If an RSVP LSP is configured for auto-bandwidth, the ingress LER determines, at every adjust interval, whether to attempt an auto-bandwidth adjustment. You can change the minimum bandwidth, maximum bandwidth, or threshold parameters on an operational LSP, however, the changes do not take effect until the next auto-bandwidth trigger, for example, an adjust interval expiry. If the bandwidth adjustment fails, for example, the CSPF cannot find a path, the existing LSP is maintained with its existing bandwidth reservation. See Procedure 32-8 for more information.

Static LSPs

A static LSP uses an IGP instead of a signaling protocol, such as LDP or RSVP-TE. The 5620 SAM attempts to derive the hop configurations based on the hop labels in the path. You must use an ingress label that is unique within an NE when you create a new static hop; otherwise, the 5620 SAM rejects the new hop.

You can assign static label mappings for LSP cross-connections on an MPLS interface during interface creation or modification. A static label map is used only for intervening unmanaged NEs. The 5620 SAM attempts to derive the interface and label values from the swap egress label of the previous hop. The Static Label Maps form lists the static label maps for an interface whether they are created using the 5620 SAM client GUI, an OSS client, or CLI.

The 5620 SAM does not raise an alarm against an unmanaged NE.

The 5620 SAM raises an alarm against a static LSP under the following conditions when the LSP destination is managed by the 5620 SAM:

- No hops are configured for the static LSP.
- The last hop does not match the LSP destination.
- The label action specified for the last hop is not a pop action.

Point-to-Multipoint LSPs

A Point-to-Multipoint (P2MP) MPLS LSP allows the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network. A P2MP LSP tree is established in the control plane for which the path consists of a head-end node, one or many branch nodes, and multiple leaf nodes. Packets that are injected by the head-end node are replicated in the data plane at the branching nodes before they are delivered to the leaf nodes.

The P2MP LSP has a source IP address but does not a have a destination address. Instead, you must create S2L Leaf nodes for each destination in the P2MP LSP tree. The P2MP LSPs are not supported in SDP bindings.

Each P2MP LSP object has one P2MP LSP Instance object. This is the primary instance, and can hold multiple child S2L Paths objects. Just as the P2MP LSP can appear as a tree, each S2L Path object then represents a root-to-leaf (S2L) sub-LSP path for the primary instance. The S2L Paths can be empty paths, or can specify a list of explicit hops. The same path can be used by more that one S2L of the instance. However the destination IP address must have a unique argument per S2L, because it corresponds to the address of the egress LER node.

PIM tunnel interfaces are associated with a P2MP LSP. The tunnel interfaces are needed at both the ingress LER and the egress LER nodes. You must also associate static multicast groups to the tunnel interfaces that are associated with the P2MP LSPs.

On the ingress side, you can create one or more tunnel interfaces in PIM and associate each with a different RSVP P2MP LSP. The tunnel interface is associated with the P2MP LSP name. You can then assign static multicast group joins to each tunnel interface using an IGMP configuration. A specific <*,G> or <S,G> can only be associated with a single tunnel interface. A multicast packet which is received on an interface and matches the <*,G> or <S,G> specified in the IGMP join for the tunnel interface is replicated and forwarded to all branches of the P2MP LSP.

On the egress side, the PIM tunnel interface is associated with both the P2MP LSP name and the system address of the ingress LER. You must define a multicast info policy to associate specific multicast groups, or a specific <S,G>, to the primary tunnel interface on each egress LER leaf node. The multicast info policy must then be applied to the router. A multicast packet synced from a tunnel interface associated with a P2MP LSP on the egress leaf node can then be forwarded over a PIM or IGMP interface, which can be an access interface or a network interface, including a spoke SDP-based IES interface. You may create multiple tunnel interfaces per node, where each interface is associated with a different P2MP LSP. The P2MP LSP association to a multicast group can be applied at the bundle, channel, and/or source channel level in the policy.

You can create a P2MP LSP using the LSP template for MVPN from the Policies→MPLS→LSP Template MVPN menu option. You can configure the scope as either local or global. The global template can be modified and multiple local versions can exist on the NEs. You must assign a default MPLS path to the template on the local definition before the template is turned up. If you modify the template, you must shut down the local policy first. When you turn up the local policy, all previously created P2MP LSP parameters are synchronized with the new template. See Procedure 32-23 for more information.

Bypass LSPs and manual bypass tunnels

You can create manual bypass tunnels and dynamic (or automatic) bypass tunnels on the SR/ESS, 7705 SAR, and 7210 SAS. You can manually configure an LSP to be bypass-only on a PLR node. The LSP is then used exclusively for the purpose of bypass protection.

You can use manual bypass alone or with dynamic bypass. When used with the dynamic bypass, the manual bypass has precedence over the dynamic bypass for the path selection.

Dynamic bypass tunnels can be disabled on a per node basis. They are enabled by default. If dynamic bypass is disabled on a node while dynamic bypass tunnels are active, traffic loss occurs. Furthermore, if no suitable manual bypass LSPs are found, the protected LSP remains without protection.

A bypass-only LSP does not have all the configurable attributes of a regular dynamic LSP. The main differences include:

- Manual bypass LSPs only support primary path. No secondary or standby paths can be created.
- Manual bypass LSPs do not support bandwidth or fast-reroute.
- Path monitoring is not available for manual bypass LSPs.
- Manual bypass LSPs cannot be assigned to a service tunnel, or be added to an LDP targeted peer as the LDP tunnelling LSP.
- There is no rule-based topology support available for manual bypass LSPs.
- There is no network-wide LSP view (the physical map LSP view) support available for manual bypass LSPs,
- You cannot create a static LSP using a tunnel template.

The following additional characteristics also apply to a manual bypass:

- The default protection level for a bypass tunnel is “node-protect”.
- CSPF is supported for the manual bypass tunnel. When CSPF is enabled, loose path and hop-less path are allowed on a manual bypass tunnel. The CSPF calculation is performed when the manual bypass tunnel is first set up.

Tunnel Templates

Tunnel templates allow users to configure dynamic LSP, LSP path, and SDP templates to define common characteristics for a tunnel or templatable tunnel object. Configure tunnel templates to reduce configuration time. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel XML API templates.

To simplify creating tunnel templates, the 5620 SAM provides examples of common tunnel templates that can be copied and customized. You can also create a tunnel template from an existing templatable object. See the *5620 SAM Scripts and Templates Developer Guide* for information about using tunnel template examples and creating a tunnel template from an existing object.

After a template is configured, dynamic LSPs, LSP paths and SDPs can be configured by choosing a create from template button during configuration. Users can configure multiple LSP paths for a dynamic LSP. For example you can configure one primary, one standby, and many secondary LSP paths.

When the 5620 SAM auto-tunnel creation is used to create LSP paths, the LSP paths must use a hopless path. If the paths belong to the same LSP, they must use different MPLS paths, even when the MPLS paths are hopless. For a RSVP LSP policy, one LSP template can be specified. When an LSP template with multiple LSP paths is specified, many LSP paths are created.

LSP Path Optimization Policy

The 5620 SAM allows you to resignal LSP Paths to take advantage of new paths that are less congested, fewer hops, have a lower metric and meet least-fill criteria. NEs periodically check the network to determine whether a more efficient path is available and notify the 5620 SAM when another path is eligible for re-signalling. 5620 SAM maintains a list of LSP Paths that are eligible for re-signaling. When a LSP Path is eligible for optimization, the LSP Path can be routed to a different path. When a LSP Path not eligible for optimization, the LSP Path cannot use newly available network resources.

A LSP Path optimization policy allows the operator to filter the LSP Path candidates and set the execution rules to determine the candidacy and priority of an LSP Path for re signalling. The 5620 SAM operator can define LSPs Paths that are eligible for re-signaling and if a path is selected, the LSP Path is added to a candidate list. Execution rules determine the sequence in which the LSP Paths can re-signal and the number of seconds between re-signalling. Execution rules apply to the entire candidate list. Each time that optimization starts, the candidate list is filtered according to the candidate definition values and then re sequenced according to the sequencing target and order values.

To ensure that NEs are not overloaded by LSP re-signaling, an LSP Path optimization schedule can be created to identify when re-signaling can be evaluated and executed. You can also manually execute LSP Path optimization schedules. To avoid network congestion and maintain QoS standards, one policy should be executed at a time. Repetitive re-signaling requests are ignored, including manual or scheduled re-signaling requests. However, a re-signaling request that is initiated from the LSP Path binding properties window executes regardless of whether another LSP optimization policy is in progress.

The NEs notify the 5620 SAM about the current state and outcome of LSP Path re-signaling. You can access the LSP Path property window to view information about the state of LSP Path optimization. The following parameters are displayed:

- The Resignal Eligible parameter indicates whether a LSP Path is eligible for optimization. When the parameter value is true, the LSP Path can be optimized. When the parameter value is false, the LSP Path is not eligible for optimization.
- The Last Performed Type parameter indicates how resignaling was performed. Typically the value is Manual Resignal. However, if a schedule was set, the value is Timer Based Resignal.
- The Last Performed parameter indicates the last time the LSP Path was chosen to be re-signaled.
- The Last Performed State parameter indicates the re-signal state of a specific LSP Path.

LDP-over-RSVP tunnels

In networks that contain dozens of NEs spanning multiple routing areas, many RSVP service tunnels may be required. To reduce the number of RSVP tunnels required for service deployment in large networks, you can use the 5620 SAM to create LSPs using LDP-over-RSVP, sometimes called tunnel-in-tunnel encapsulation. An SDP can ride on multiple LDP-over-RSVP tunnels.

The 5620 SAM supports automatic, rule-based service-tunnel creation using NEs that are grouped according to their role in the 5620 SAM-managed network. This functionality greatly reduces the time and effort required to provision a mesh of service tunnels. See chapter 33 for more information about rule-based automatic service-tunnel creation.

The 5620 SAM can use tunnel rules and groups to create new RSVP LSP bindings between a PE device that is added to the network and the existing ABRs. It can also create a new LDP-over-RSVP tunnel between a new NE and an existing PE NE. See chapter 33 for more information about tunnel creation using rules and groups.

Service traffic that is transported by an LDP-over-RSVP tunnel requires a VC label, an LDP label, and an RSVP label. Unlike T-LDP sessions that use IGP SPF algorithms, RSVP LSPs are not advertised to an IGP instance. When the same FEC applies to the destination of an LDP-over-RSVP LSP tunnel and an IGP-based LDP tunnel, the 5620 SAM uses the LDP tunnel by default to minimize network overhead.

Using tunnel-in-tunnel encapsulation, a pair of LSP tunnels and a T-LDP session between two NEs are equivalent to two adjacent LDP NEs with a non-tunneled LDP session between them. In other words, the LDP tunnel uses the RSVP LSP as one hop between LSRs in the network.

During the configuration of LDP-over-RSVP, you can specify an explicit list of dynamic and static LSPs, or use the 5620 SAM to find eligible LSPs. After an LSP is explicitly configured for LDP tunnelling, the 5620 SAM associates the LDP targeted peer with the LSP.

You can configure LDP-over-RSVP to enable an OSPF area router to be a stitching point. You can specify which NEs to use as the stitching points in each area. When there are many NEs in an area, this function helps to reduce the number of LSPs required, because a full mesh is not required.

For an LSP to be eligible for LDP-over-RSVP, the following conditions apply:

- The LSP must be an RSVP-owned LSP (strict or loose)
- The LSP must start and terminate either on:
    - The router ID (system IP address)
    - The router ID (loopback address when used in multi-instance OSPF
- The OSPF system/loopback address must be advertised
- A T-LDP session must exist between the originating and terminating routers using the addresses cited above
- LDP-over-RSVP availability must be enabled in the LSP configuration. This indicates that the LSP is eligible for LDP-over-RSVP, and RSVP signals to the IGP that the LSP should be included in the SPF run.

Shared Risk Link Groups

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. Firstly, you can establish a FRR LSP path. In addition, you can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. Links which are members of the same SRLG represent resources which are assumed to share the same risk. These links are therefore avoided when computing and setting up an alternate LSP path.

- FRR backup

  The SRLG constraint can be enabled system-wide on a PLR node, in the computation of a FRR detour or bypass to be associated with a primary LSP path. CSPF includes the SRLG constraint in the computation of a FRR detour or bypass. CSPF then prunes all links with interfaces which belong to the same SRLGs as the egress interface being protected (or the immediate downstream node, depending on the protection level). If a path is found, the bypass or detour is set up. If not, and you included the Enable SRLG for FRR - Strict option, then the bypass or detour is not set up. If the Enable SRLG for FRR - Strict option is not specified, and a path exists that meets other TE constraints (other than the SRLG constraint), then the bypass or detour is still set up.
- Secondary LSP backup

  The SRLG constraint can also be enabled per LSP path on a head-end LER in the computation of an LSP secondary path that includes the standby path. The SRLG constraint is additional to the admin group constraint on the same secondary LSP path. CSPF includes the SRLG constraint in the computation of the secondary LSP path, which requires that the primary LSP path is configured and active. CSPF prunes links with interfaces that belong to the same SRLGs as the interfaces included in the primary path. If a path is found, the secondary LSP path is set up. Otherwise, CSPF keeps trying to set up the secondary LSP path.

You can enable only the SRLG constraint for the FRR backup operation. However, you can enable both the SRLG constraint and the admin-group include/exclude constraint for the secondary LSP backup path operation. In either case, you can still apply the admin-group constraint for the primary path.

The following conditions also apply to SRLGs:

- An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution and resynchronization
- SRLGs are defined node wide
- Configured SRLGs are associated with MPLS interfaces. A specific MPLS interface can belong to multiple SRLGs. Up to 64 SRLGs can be associated with a specific MLPLS interface

Bandwidth-based equal cost RSVP LSP path selection

When multiple equal-cost paths satisfy the constraints of a specific RSVP LSP path, CSPF in the 7x50 head-end node uses a random number generator to select a path and return it to MPLS. While this method actually balances the number of LSP paths over the links in the network, it does not necessarily balance the bandwidth utilization across those links.

In order to achieve load balancing of the bandwidth amongst the available LSP paths, CSPF must include the link utilization as a criterion in the path selection. One algorithm that considers this is referred to as the "least-fill" path selection. This algorithm identifies the single link in each of the equal-cost paths that has the least available bandwidth in proportion to its maximum reservable bandwidth. CSPF then selects the path containing the link with the largest such available bandwidth to maximum reservable bandwidth percentage. The net effect of using this algorithm is that over time, LSP paths become spread over the network links in such a way that the percentage of link utilization is balanced.

When comparing the percentages of least available link bandwidth across the sorted paths, if two percentages differ by less than a value you configure as a minimum threshold, CSPF considers them equal. It then applies a random number generator to select amongst these paths. You can also specify a reoptimization threshold, which allows you include a path cost consideration into the decision of when to alter the paths used by the LSP.

LSP on-demand resynchronization

LSP on-demand resynchronization is supported on the 7750 SR and 7710 SR. You can modify the nms-server.xml file to allow a user to manually resynchronize an LSP. On-demand resynchronization does not affect the existing manual full node resynchronization functionality. However, when LSP on-demand resynchronization is enabled, any scheduled resynchronization is blocked for the following LSP objects:

- RSVP session
- cross-connect
- in-segment
- out-segment
- actual hop
- CSPF hop

Therefore, these LSP objects are not resynchronized as a result of a relevant trap. The exception is that for 5650 CPAM path monitored LSPs, the actual hop trap (a generic trap) is still processed.

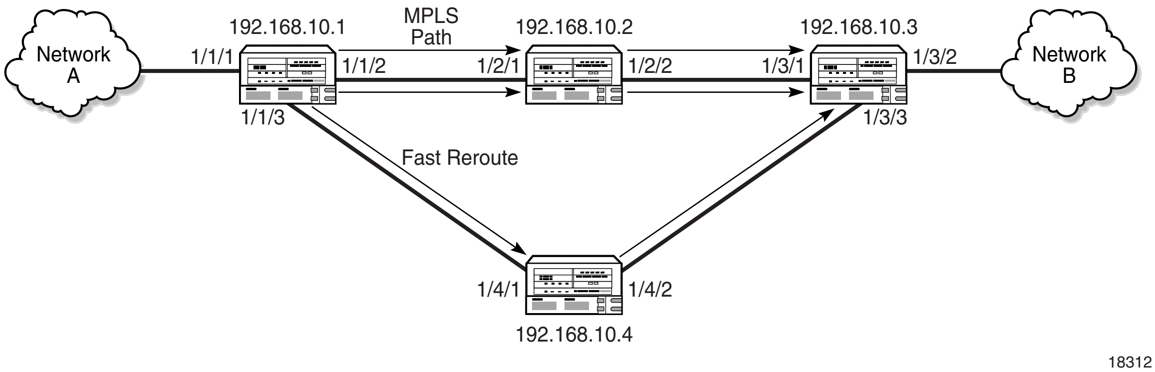
By default, the LSP on-demand resynchronization functionality is disabled. See chapter 6 for information about how to enable LSP on-demand resynchronization. After you enable LSP on-demand resynchronization, click on the Resync button on the LSP configure form to start the manual LSP on-demand resynchronization. The following objects are resynchronized, depending on the type of LSP:

- for a dynamic LSP: the LSP, LSP path, CSPF and actual paths, bypass or detour path, cross-connects, in-segments, out-segments, and RSVP sessions
- for a manual bypass LSP: the LSP, LSP path, CSPF and actual paths, cross-connects, in-segments, out-segments, and RSVP sessions
- for a static LSP: the head-end LSP, the static hops, static label maps, cross-connects, in-segments, and out-segments. You must manually resynchronize all of the planned hop sites in a static LSP before creating a static LSP.

32.2 Sample MPLS configuration

Figure 32-1 shows an example of an MPLS service configuration. The actual configuration depends on the specific network requirements.

Figure 32-1 Sample MPLS configuration



The high-level tasks that are required to configure the MPLS service example in Figure 32-1 follow.

Preconfiguration

1 Before you begin, verify that the following preconfigurations have been made.

- An IGP is enabled on all participating NEs and includes the system interface in the IS-IS or OSPF area.
- Any additional Layer 3 interfaces that you wish to use are configured.

Configuration

2 Create an MPLS path as follows:

i Specify 192.168.10.1 as the source network element.

ii Specify 192.168.10.2 and 192.168.10.4 as hops.

iii Specify interface 1/3/2 on 192.168.10.3 as the destination site. This is the final hop in the MPLS path.

3 Create a dynamic LSP as follows:

i Specify interface 1/1/1 on 192.168.10.1 as the source IP address.

ii Specify 192.168.10.3 as the destination IP address.

4 Bind the dynamic LSP created in step 3 to the MPLS path created step 2.

32.3 Workflow to configure MPLS

1. Enable and configure one or more IGPs such as IS-IS, RIP, and OSPF to include the system interface on all NEs that are to participate in the MPLS network. See the appropriate device documentation for more information.

2. Enable MPLS on the routing instances of all NEs that are to participate in the MPLS network. See Procedure 32-1 for more information.

3. Create or configure an MPLS instance. Assign Layer 3 interfaces, including the system management interface, to the MPLS instance. See Procedure 32-2 or Procedure 32-3 for more information.

4. Create a mesh of MPLS paths. See Procedure 32-4 for more information.

5. Create a mesh of LSPs.

    a. Create a static LSP. See Procedure 32-6 for more information.

    b. Create a dynamic LSP. See Procedure 32-8 for more information. See Procedure 32-9 for more information on creating a dynamic LSP from a tunnel template.

    c. Create a Point-to-Multipoint LSP. See Procedure 32-14 for more information.

    d. Create a Manual Bypass LSP. See Procedure 32-15 for more information.

    e. Create a mesh of LSPs on a 7250 SAS device.

        i. Create a guarding LSP. See Procedure 32-10 for more information.

        ii. Create a dynamic LSP. See Procedure 32-11 for more information.

6. If your mesh includes dynamic LSPs or bypass-only LSPs, configure an LSP path. See Procedure 32-17 or Procedure 32-18 for more information.

7. If required, create an LSP Path optimization policy. See Procedure 32-19 for more information.

Note 1 — Only static LSPs and static FRR LSPs are supported on the OS 9700E and OS 9800E NEs.

Note 2 — RSVP is not supported on the OS 9700E and OS 9800E NEs.

Note 3 — Label actions cannot be modified on NEs after the labels are created by the 5620 SAM.

32.4 MPLS procedures

Use the following 5620 SAM procedures to manage MPLS.

Procedure 32-1 To enable MPLS on a routing instance

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to a routing instance. The path is Routing→NE→Routing Instance.

3 Right click on the routing instance and choose Properties from the contextual menu. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab button.

5 Select the MPLS Enabled parameter. RSVP is enabled by default and cannot be disabled using the 5620 SAM.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Routing Instance (Edit) form closes.

The 5620 SAM creates an MPLS instance and displays it below the routing instance in the navigation tree.

Procedure 32-2 To configure an MPLS instance

Note 1 — The MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, must be enabled using the CLI.

Note 2 — The only parameter that you can configure on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, is the Dynamic Bypass parameter.

Note 3 — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the site level:

- General
- Interfaces
- In Segments
- Cross Connects
- Out Segments
- Static Label Maps
- Faults

1 Enable MPLS on an NE, as described in Procedure 32-1.

2 Choose Routing from the 5620 SAM navigation tree view selector.

3 Navigate to an MPLS instance. The path is Routing→NE→Routing Instance→MPLS.

4 Right-click on the MPLS icon in the navigation tree, and choose Properties from the contextual menu. The MPLS (Edit) form opens with the General tab displayed.

5 Configure the parameters.

- Administrative State
- Fast Reroute
- Dynamic Bypass
- Static LSPs Fast Retry Timer (seconds)
- Exponential Backoff Retry
- Maximum Bypass Associations
- In the LSP Resignal panel:
  - Enable
  - Resignal Timer (min)
- In the P2MP LSP Resignal panel:
  - Enable
  - Resignal Timer (min)
- In the Hold Timer panel:
  - Enable
  - Hold Timer (seconds)
- In the Shared Risk Link Group panel:
  - Enable SRLG for FRR
  - Strict
- In the Least-Fill panel:
  - Least Minimum Threshold
  - Least Reoptimization Threshold
- In the TTL Propagate panel:
  - Shortcut Local TTL Propagate
  - Shortcut Transit TTL Propagate
- In the Auto Bandwidth Multipliers panel:
  - Sample Multiplier
  - Adjust Multiplier
- In the Inter Area/Level Traffic Engineering panel:
  - CSPF On Loose Hop

6 If you are configuring an MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 7. Otherwise, if you need to configure OAM diagnostics for the MPLS instance, click on the Tests tab button. See chapter 38 for more information about configuring OAM diagnostics.

7 To configure MPLS interfaces on the MPLS instance, click on the Interfaces tab button. See Procedure 32-3 for more information about configuring MPLS interfaces. If you are configuring an MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 14.

8 To configure the collection of ingress accounting statistics for the MPLS instance, click on the Accounting tab button.

9 Click on the Create button. The , Routing Instance (Create) form opens.

10 Configure the parameters in the LSP Information block:

- LSP Name
- Sender Address

11 Configure the parameters in the Ingress Accounting Statistics block:

- Click on the Select button. The Select Accounting Policy - IngStatsPolicy - Routing Instance form opens. Choose the required accounting policy and click on OK. Only accounting policies with the CombinedMplsLspIngressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

Note — The collection of egress accounting statistics is configured in Procedure 32-8.

See the 5620 SAM Statistics Management Guide for more information on the collection of statistics.

12 Click on the following tab buttons to view information about the MPLS instance, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Static Label Maps to view static hop mapping information
- Statistics to view MPLS site and interface statistics
- Faults to view alarm information for the MPLS instance

13 Click on the More Actions button and choose View RSVP Site to view the associated RSVP instance on the NE.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The MPLS (Edit) form closes.

Procedure 32-3 To create an MPLS interface

Perform this procedure to create an MPLS interface by assigning a network interface to an MPLS instance.

This procedure requires the existence of an L3 network interface on the NE that hosts the MPLS instance. See section 30.1 for more information about configuring network interfaces.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the interface level:

- General
- In Segments
- Static Label Maps
- Cross Connects
- Out Segments
- Faults

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to an MPLS instance icon. The path is Routing→NE→Routing Instance→MPLS.

3 Right-click on the MPLS icon and choose Create Interface from the contextual menu. The MPLS Interface (Create) form opens with the General tab displayed.

4 Assign an L3 network interface as the MPLS interface.

i Click on the Select button. The Select Interface form opens.

ii Choose an interface from the list and click on the OK button.The interface is displayed in the Interface panel on the MPLS Interface (Create) form.

5 Configure the parameters:

- Description
- Administrative State

If you are creating an MPLS interface on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to 7.

6 In the TE Metric block, configure the parameters:

- TE Metric Enabled
- TE Metric

7 Click on the Apply button. The form displays additional tabs, and the 5620 SAM creates the MPLS interface and displays it below the MPLS instance in the navigation tree.

If you are creating an MPLS interface on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to 10.

8 Configure a Shared Risk Link Group, if required.

i Click on the Shared Risk Link Groups tab button. The Shared Risk Link Group list page opens.

ii Click on the Create button. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form opens.

iii Click on the Search button. The available SRLGs are displayed.

iv Select the required SRLGs and click OK. Up to 64 SRLGs can be associated with a specific MPLS interface. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form closes and the selected SRLG is displayed in the Shared Risk Link Group list page.

9 Configure a static label map, if required. A static label map is required when there are intervening unmanaged NEs between the managed NEs in an MPLS path.

Note — Alcatel-Lucent recommends that you use a static label mapping only to specify unmanaged NEs.

i Click on the Static Label Maps tab button.

ii Click on the Create button. The Static Label Map (Create) form opens. Alternatively, you can choose a Static Label Map from the list and click on the Properties button to edit the Static Label Map properties.

iii Configure the Label Action parameter. When you change the Label Action parameter from unspecified to Pop or Swap, the Static Label Map (Create) form changes to include other parameters. Configure the other parameters as required:

- Ingress Label
- Egress Label
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Next Hop
- Administrative State

The Egress Label, Next Hop and Enable Implicit Null Label parameters are only configurable when the Label Action parameter value is set to Swap.

The Egress Label and Next Hop parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

The 5620 SAM sets the Label Action parameter value to Pop when the hop destination matches the destination LSP.

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

10 Click on the Administrative Groups tab button to assign MPLS administrative groups to the interface, as required. After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

11 Click on the following tab buttons to view information about the MPLS interface, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Statistics to view the MPLS site and interface statistics
- Faults to view alarm information for the MPLS interface

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The MPLS Interface properties form closes.

Procedure 32-4 To create an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Click on the Create button. The Create MPLS Path form opens with the Name the MPLS Path step displayed.

3 Configure the parameters.

- Name
- Description

4 Click on the Next button. The Define Source Site step displayed.

5 Perform one of the following actions to specify a 5620 SAM-managed NE for the Starting Network Element parameter value.

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Select Source Site form opens.

ii Select an NE in the list and click on the OK button. The management IP address of the NE is displayed as the source site of the MPLS path.

b Enter the management IP address of the port.

6 Click on the Next button. The Define the provisioned Path step is displayed.

7 Click on the Insert Hop button to insert an MPLS path hop. The Hop for New MPLS Path (Create) form opens.

8 Configure the Specify Site parameter. Perform one of the following actions.

a Specify the IP address of an unmanaged NE.

i Choose Manually.

ii Configure the IP Address parameter.

b Select a managed NE.

i Choose By Selection.

ii Click on the Select button. The Select a Network Element - New MPLS Path form opens.

iii Select an NE in the list and click on the OK button. The management IP address of the NE is displayed as the Name and IP Address values.

iv Specify an alternative interface on the NE to be used as the hop point, if required, by manually configuring the IP Address parameter.

9 Configure the Hop Type parameter.

Note — The Hop Type parameter is set to a value of strict and is not configurable for any of the hops on a path that originate from or terminate on a 7250 SAS-ES 2.0.

10 Click on the Apply button.

11 Insert an additional hop, if required, by repeating steps 8 to 10.

12 Click on the OK button. The Create MPLS Path form reappears.

13 To change the hop sequence, choose a hop and click the Move Up or Move Down button. The first hop in the list is the first hop, and the last hop in the list becomes the destination site when the form changes are saved.

14 Click on the Next button. The Set Initial State step is displayed.

15 Configure the Administrative parameter. This parameter is set to Up and is not configurable if the path originates on 7250 SAS-ES or 7250 SAS-ESA NEs.

16 Click on the Finish Button to save the configuration. You are prompted to view the MPLS path.

17 Enable the View the newly created MPLS path parameter to view the MPLS path configuration after closing the form, if required.

18 Click on the Close button. The Create MPLS Path form closes.

19 If the View the newly created MPLS path parameter in step 16 is enabled, the MPLS Path (Edit) form opens with the newly created MPLS path configuration displayed.

i View the configuration, if required.

ii Close the MPLS Path (Edit) form.

20 Close the Manage MPLS Paths form.

Procedure 32-5 To view an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Configure the filter criteria. A list of MPLS paths is displayed.

3 View the MPLS path information as required. The information includes the following:

- name and description
- ID
- source and destination sites
- administrative and operational states

Procedure 32-6 To create a static LSP

Note — When LSP on-demand resynchronization is enabled, manually resynchronize all of the planned hops in the static LSP before you create a static LSP. This is to ensure that validations on the static LSP can be run properly. See chapter 6 for information about enabling LSP on-demand resynchronization.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Click on the Create button. The Static LSP (Create) form opens.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Source Site ID
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Administrative
- Destination Site ID

Note 1 — If a range policy is applied to a service tunnel, a grey text box appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation, to indicate that a format policy is enforced. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to select a policy. The items in the combo box are ordered by the policy's Priority parameter.

Note 2 — The Administrative parameter applies to the source NE only, not to the entire static LSP

4 Click on the Static Hops tab button.

5 Click on the Create button. The Static Hop (Create) form opens.

6 Configure the Hop Index parameter.

7 Click on the Select button in the Site panel to configure the Site ID parameter. The Select Site - Static Hop form opens with a list of the available hop sites.

8 Select a site in the list and click on the OK button. The Select Site - Static Hop form closes and the Static Hop (Create) form displays the site information.

9 Click on the Select button in the Interface panel to configure the Interface Name parameter. The Select Interface - Static Hop form opens with a list of the available interfaces on the hop site.

10 Select an interface in the list and click on the OK button. The Select Interface - Static Hop form closes and the Static Hop (Create) form displays the interface name.

11 Configure the parameters.

- Label Action
- Ingress Label
- Egress Label
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Next Hop
- Administrative State

The Egress Label, Enable Implicit Null Label and Next Hop parameters are configurable when the Label Action parameter value is set to Swap.

The Egress Label and Next Hop parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

12 Click on the OK button. The Static Hop (Create) form closes and a dialog box appears.

13 Click on the OK button. Static LSP (Create) form reappears.

14 Insert an additional hop, if required, by repeating steps 5 and 13.

15 Click on the OK button. The Static LSP (Create) form closes and a dialog box appears.

16 Click on the Yes button. The Static LSP (Create) form closes and the Manage Static LSPs form reappears.

17 Close the Manage Static LSPs form.

Procedure 32-7 To view and configure a static LSP

The following procedure applies only to the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, and 7710 SR. See the device documentation for related information specific to the 7250 SAS-ES and 7250 SAS-ESA if required.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of static LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Static LSP (Edit) form opens.

4 Click on the following tab buttons to view information about the static LSP, as required.

- Static Hops to view and configure LSP hops
- Service Tunnels to view a list of service tunnels associated with the static LSP
- LDP Tunneling to view a list of LDP-over-RSVP tunnels associated with the static LSP
- Statistics to view the static LSP site and interface statistics
- Faults to view alarm information for the static LSP

5 Close the Static LSP (Edit) form.

6 Close the Manage Static LSPs form.

Procedure 32-8 To create a Dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID
- Preference

Note — When a range policy is applied to a dynamic LSP, a dimmed text field appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a dynamic LSP, a combo box appears beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to select a policy. The sequence of the options in the combo box are specified by the policy Priority parameter.

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also manually specify an IP address for each parameter in this step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Select a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter value. This parameter is automatically populated with the system IP address of the site.

iii Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Select a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path form opens.

7 Configure the parameters.

- Auto Select Hop-less Path
- Reserved Bandwidth (Mbps)

The Reserved Bandwidth (Mbps) parameter is configurable when the Auto Select Hop-less Path parameter is enabled.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The Add MPLS Paths form opens. This step binds the LSP to the MPLS path to create an MPLS path.

i Configure the Termination Validation parameter.

ii Click on the Create button. The LSP-Path Binding form opens with the Choose Path Type step displayed.

iii Configure the Type parameter.

iv Click on the Next button. The Choose MPLS Path step is displayed. Select an MPLS path in the list to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

v Click on the Next button. The Set Traffic Options form opens.

vi Configure the parameters.

- Reserved Bandwidth (Mbps)
- Inherit Value
- Hop Limit
- Record Actual Path
- Path Preference

The Path Preference is only configurable on Standby LSP paths (Type parameter set to standby).

vii Click on the Next button. The Set Initial States form opens.

viii Configure the Administrative parameter.

ix Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

x Click on the OK button. The Create Dynamic LSP form reappears.

10 Click on the Next button. The Properties - Traffic Engineering and Protection step is displayed.

11 Configure the parameters.

- Fast Reroute
- Hop Limit
- IGP Shortcut Enabled
- BGP RSVP LSP Transport Tunnel
- BGP Shortcut Enabled
- Diff-Serv Class Type
- Main Class Type Retry Limit

12 Click on the Next button. The Properties - Fast Reroute step is displayed.

13 Configure the parameters:

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect

14 Click on the Next button. The Properties - Signalling step is displayed.

15 Configure the parameters.

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

16 Click on the Next button. The Properties - Make before Break step is displayed.

17 Configure the Make before Break parameter.

18 Click on the Next button. The Properties - CSPF form opens.

19 In the CSPF block, configure the parameters:

- Enable CSPF
- Enable TE Metric
- Inter Area CSPF To First Loose Hop

20 Click on the Next button. The Properties - Route Selection step is displayed.

21 Configure the parameters:

- Metric
- Least-Fill Path Selection

The Least-Fill Path Selection parameter can only be enabled when the Enable CSPF parameter is enabled in step 19.

22 Click on the Next button. The Properties - Administrative Groups step is displayed.

23 Assign one or more MPLS administrative groups to the dynamic LSP.

i Select the required MPLS administrative groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the dynamic LSP and moved to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

24 Configure the Propagate Admin Group parameter.

25 Click on the Next button. The Properties - LDP Tunneling step is displayed.

26 Configure the LDP over RSVP include parameter.

27 Click on the Next button. The Properties - Auto-Bind step is displayed.

28 Configure the Enable Auto-Bind parameter.

Note — The Enable Auto-Bind parameter is configurable only on a 7710 SR or 7750 SR.

29 Click on the Next button. The Set Initial State step is displayed.

30 Configure the Administrative parameter.

31 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

32 Enable the View the newly created Dynamic LSP parameter to view the dynamic LSP configuration after closing the form, if required.

Note — If you enable the View the newly created Dynamic Lsp parameter you can configure the collection of egress accounting statistics using the dynamic LSP configuration form.

33 Click on the Close button. The Create Dynamic LSP form closes.

34 If the View the newly created Dynamic LSP parameter is enabled in step 32, the Dynamic LSP (Edit) form opens with the newly created dynamic LSP configuration displayed.

i View the configuration, if required.

ii If you need to enable the collection of egress accounting statistics, go to step iv. Otherwise go to step ix.

iii If you need to configure auto-bandwidth for the dynamic LSP, go to step vi. Otherwise, go to step ix.

iv Click on the Accounting tab button.

v Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - Dynamic LSP form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedMplsLspEgressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

Note 1 — The Ingress Accounting Statistics panel displays a read-only view. If an ingress accounting statistics record exists, you can click on the Properties button to view the record.

Note 2 — The collection of ingress accounting statistics is configured in Procedure 32-2.

See the 5620 SAM Statistics Management Guide for more information on about the collection of statistics.

vi Click on the Properties tab button.

vii Set the Auto Bandwidth parameter in the Traffic Engineering And Protection panel to true to view and configure the auto-bandwidth parameters.

viii Configure the parameters in the Auto Bandwidth panel.

- Adjust Up Threshold (percent)
- Adjust Down Threshold (percent)
- Minimum Bandwidth (mbps)
- Monitor Bandwidth
- Sample Multiplier
- Overflow Limit
- Adjust Up Bandwidth (mbps)
- Adjust Down Bandwidth (mbps)
- Maximum Bandwidth (mbps)
- Adjust Multiplier
- Overflow Limit Threshold (percent)
- Overflow Limit Bandwidth (mbps)

ix Click on OK to close the Dynamic LSP (Edit) form.

35 Click on OK to close the Manage Dynamic LSPs form.

Procedure 32-9 To create a dynamic LSP from a tunnel template

Before you can create an LSP from a tunnel template, you must create the tunnel template. You can use an existing LSP to create a tunnel template. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template window opens with a list of tunnel templates.

3 Choose a template from the list.

4 Click on the OK button. A Create Dynamic LSP from Template form opens.

5 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID
- Preference
- Administrative State

6 Specify the source sites for the dynamic LSP.

i Click on the Select button beside the Source Site ID parameter. The Select Network Element form opens with a list of the available sites.

ii Choose a site from the list and click on the OK button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source site information.

iii Click on the Select button beside the Source IP Address parameter. The Select Network Element form opens with a list of the available sites.

iv Choose a site from the list and click on the Ok button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source IP address information.

7 Configure the Destination Site ID and the Destination IP Address parameters.

8 Configure the Show created object parameter.

9 Click on the Accounting tab button.

10 Click on the Select button beside the Accounting Policy parameter. A Select Policy window opens.

11 Choose a policy from the list.

12 Click on the OK button.

13 Configure the Collect Accounting Statistics and the Administrative State parameters.

14 Click on the Properties tab button.

15 Configure the parameters:

Note — The number of parameters that can be configured depends on how the template was created. All of the following parameters are configurable when the template is based on an object. A subset of the following parameters can be configured when the template is based on an object class.

- Guarding Lsp
- Guarding Lsp
- Fast Reroute
- Hop Limit
- Diff-Serv Class Type
- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Make before Break
- Enable CSPF
- Enable TE Metric
- Metric
- Least-Fill Path Selection
- Groups Included
- Groups Excluded (bitmap)
- Persistent
- Permit Merge
- Record Actual Route
- Record Label
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Backup Setup Priority
- Backup Hold Priority
- LDP over RSVP include
- Enable Auto-Bind

16 Click on the OK button. When the LSP configuration is successful, the Create Dynamic LSP from Template form closes and the Dynamic LSP (Edit) form reappears.

If the LSP configuration is unsuccessful, the Create Dynamic LSP from Template form remains open and an error message appears.

17 Close the Manage Dynamic LSPs form.

Procedure 32-10 To create a guarding LSP on a 7250 SAS device

This procedure applies to 7250 SAS-ES and 7250 SAS-ESA devices.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form appears.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also specify an IP address for each parameter in this step.

i Click on the Select button beside the Source Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Choose a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter. The parameter is automatically configured with the system IP address of the site.

iii Click on the Select button beside the Destination Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Choose a destination site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface and cannot be changed.

6 Click on the Next button. The Guarding LSP step is displayed.

7 Enable the Guarding Lsp parameter.

8 Configure the Guarded Destination parameter.

9 Click on the Next button. The Add MPLS Paths step is displayed.

i Configure the Termination Validation parameter.

ii Click on the Create button. The LSP-Path Binding form opens with the Choose Path Type step displayed. The Type parameter is set to primary and cannot be configured.

iii Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

iv If the guarding LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, go to step 9ix.

v Click on the Next button.The Set Traffic Engineering Parameters step is displayed.

vi Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

vii Click on the Next button. The Set Path Parameters step is displayed.

viii Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

ix Click on the Next button. The Set Initial State form is displayed.

x Configure the Administrative parameter. If the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, the Administrative parameter cannot be configured.

xi Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

xii Click on the OK button.

10 If the guarding LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 14, click on the Next button. The Properties - Session Attributes step is displayed.

11 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Route
- Record Label

12 Click on the Next button. The Properties - Path Parameters step is displayed.

13 Configure the parameters:

- Committed Rate
- Setup Priority
- Backup Setup Priority
- Peak Rate
- Hold Priority
- Backup Hold Priority

14 Click on the Next button. The Set Initial State step is displayed.

15 Configure the Administrative parameter. The Administrative parameter is set to Up and cannot be configured if the guarding LSP originates on a 3.0 NE.

16 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

17 Enable the View the newly created Dynamic LSP parameter to view the dynamic LSP, if required. Otherwise, go to step 19.

18 When the View the newly created Dynamic LSP parameter is enabled, the Dynamic LSP (Edit) form appears with the newly created dynamic LSP configuration displayed.

i View the configuration.

ii Close the Dynamic LSP (Edit) form and go to step 20.

19 Click on the Close button. The Create Dynamic LSP form closes.

20 Close the Manage Dynamic LSPs form.

Procedure 32-11 To create dynamic LSP on a 7250 SAS device

This procedure applies to 7250 SAS-ES and 7250 SAS-ESA devices.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form appears.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also specify an IP address for each parameter in this step.

i Click on the Select button beside the Source Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Choose a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter. The parameter is automatically configured with the system IP address of the site.

iii Click on the Select button beside the Destination Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Choose a destination site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Guarding LSP step is displayed.

7 Click on the Next button. The Add MPLS Paths... step is displayed.

8 Configure the Termination Validation parameter.

9 Click on the Create button. The LSP-Path Binding form opens with the Choose Path Type step displayed. You cannot configure the Type parameter, the value is set to primary.

10 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

11 If the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 25.

12 Click on the Next button. The Set Initial State step is displayed.

13 Configure the Administrative parameter. The Administrative parameter is set to Up and cannot be configured.

14 Click on the Finish button. The LSP-Path Binding closes and a dialog box appears.

15 Click on the Yes button. The Create Dynamic LSP form is displayed.

16 Click on the Next button. The Properties - Traffic Engineering and Protection step is displayed.

17 Configure the Fast Reroute parameter. If you selected False, go to step 20.

18 Click the Next button. The Properties - step is displayed.

19 Configure the Hop Limit parameter. The Backup Type parameter is displayed but is not configurable.

20 Click on the Next button. The Properties - Session Attributes step is displayed.

21 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Route
- Record Label

These parameters are read-only when the LSP originates from a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, and the Fast Reroute parameter is True.

22 Click on the Next button. The Properties - Path Parameters step is displayed.

23 Configure the parameters:

- Committed Rate
- Setup Priority
- Backup Setup Priority
- Hold Priority
- Peak Rate
- Backup Hold Priority

24 Go to step 48.

25 Click on the Next button. The Set Fast Reroute step opens.

26 Configure the Fast Reroute parameter. If you selected False, go to step 29.

27 Click on the Next button. The Set Fast Reroute Backup Properties step is displayed.

28 Configure the parameters:

- Hop Limit
- Backup Setup Priority
- Backup Hold Priority

The Backup Type parameter is displayed, but is not configurable.

29 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

30 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

The parameters are read-only when the Fast Reroute parameter is True.

31 Click on the Next button. The Set Path Parameters step is displayed.

32 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

33 Click on the Next button. The Set Initial States step is displayed.

34 Configure the Administrative parameter.

35 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

36 Click on the OK button.

37 If you do not need to add a secondary LSP path, go to step 48.

38 Click on the Create button. The LSP-Path Binding opens and the Choose Path Type step is displayed. The Type parameter is set to secondary if a primary path exists.

39 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

40 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

41 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

42 Click on the Next button. The Set Path Parameters step is displayed.

43 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

44 Click on the Next button. The Set Initial State step opens.

45 Configure the Administrative parameter.

46 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

47 Click on the OK button.

Caution — If you must delete a configured secondary LSP on a 7250 SAS, Release 3.0, you must first delete the MPLS Path entries you created in step 39. If you fail to do so, any new secondary LSP created on that 7250 SAS will inherit incorrect path information.

48 Click on the Next button. The Set Initial State step opens.

49 Configure the Administrative parameter. The Administrative parameter is Up and you cannot configure the value if the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0.

50 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

51 Enable the View the newly created Dynamic LSP parameter to view the dynamic LSP configuration, if required. Otherwise, go to step 53.

52 When the View the newly created Dynamic LSP parameter is enabled, the Dynamic LSP (Edit) form appears with the newly created dynamic LSP configuration displayed.

- i View the configuration.
- ii Close the Dynamic LSP (Edit) form, and go to step 54.

53 Click on the Close button. The Create Dynamic LSP form closes.

54 Close the Manage Dynamic LSPs form.

Procedure 32-12 To configure an LSP on a 7250 SAS device

Perform the following procedure to configure an LSP that originates on a 7250 SAS-ES or 7250 SAS-ESA device.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose an LSP in the list and click the on Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

4 Click on the LSP-Path Bindings tab button. A list of LSP paths is displayed.

5 You can add a secondary LSP path on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, if required. Otherwise, go to step 15.

6 Click on the Create button. The LSP-Path Binding opens and the Choose Path Type step is displayed. The Type parameter is set to secondary if a primary path exists.

7 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

8 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

9 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

10 Click on the Next button. The Set Path Parameters step is displayed.

11 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

12 Click on the Next button. The Set Initial States step opens.

13 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

14 Click on the OK button.

15 Choose an LSP path in the list and click on the Properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

16 Configure the parameters.

- Type
- Administrative
- Setup Priority
- Hold Priority
- Fast Reroute
- Backup Type
- Hop Limit
- Record Actual Path
- Record Label
- Persistent
- Permit Merge
- Backup Setup Priority
- Backup Hold Priority
- Enable CSPF

The configurable parameters depend on:

- the type of LSP path
- the software version of the originating NE
- whether fast reroute is enabled

17 Click on the Administrative Groups tab button.

18 Assign an MPLS administrative group to the LSP path.

i Choose an MPLS administrative group in the Unassigned list.

ii Click on the right arrow button. The group is assigned to the LSP path and moves to the Assigned list.

19 View a list of hops, if required.

i Click on the following tab buttons to list the path hops:

- Provisioned Path
- Actual Path

ii Click on the Topology View button to view the topology map for the path. See chapter 5 for information about using topology maps.

20 Click on the OK button. The LSP-Path Binding (Edit) form closes.

21 Click on the OK button. The Dynamic LSP (Edit) form closes.

Procedure 32-13 To list dynamic LSPs

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria. A list of dynamic LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 To view LSP path information:

i Click on the LSP Paths tab button.

ii Double-click on an LSP path in the list.

iii Review the state information.

LSP path information includes whether the bypass tunnel for the LSP is active, or whether the LSP is in a fast reroute state.

Procedure 32-14 To create a Point-to-Multipoint LSP

1 Choose Manage→MPLS→Point-to-Multipoint LSPs from the 5620 SAM main menu. The Manage Point-to-Multipoint LSPs form opens.

2 Click on the Create button. The P2MP LSP (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Name
- ID
- Auto-Assign ID
- P2MPId
- Administrative
- System ID (Loopback IP Address)
- IP Address

When you configure the System ID (Loopback IP Address) parameter, the Management IP Address and Site Name parameters are automatically populated with the values associated with that node. The IP Address parameter is also automatically populated, however, you can specify a new value for the parameter, if required.

4 Click on the Properties tab.

5 Configure the following parameters in the Traffic Engineering and Protection panel.

- Fast Reroute
- Hop Limit
- Diff-Serv Class Type

6 Configure the following parameters in the Fast Reroute panel.

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect

The Node Protect parameter is only configurable when the Reserved Bandwidth (Mbps) parameter is set to a value greater than 0.

7 Configure the Make before Break parameter.

8 Configure the following parameters in the CSPF panel.

- Enable CSPF
- Enable TE Metric

9 Configure the following parameters in the Signalling panel.

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

10 Click on the P2MP Primary Instance tab.

11 Click the Create button. The P2MP Instance (Create) form opens on the General tab.

12 Configure the parameters.

- Name
- ID
- Auto-Assign ID
- Administrative

13 Click on the Properties tab.

14 Configure the following parameters in the Traffic Engineering Properties panel.

- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Record Label

When you enable the Inherit Value parameter, the Hop Limit parameter for the P2MP Instance is set to the same value as you configured for the parent P2MP LSP.

15 Configure the following parameters in the Make Before Break panel.

- Make before Break
- Inherit Value
- Resignal

When you enable the Inherit Value parameter, the Make before Break parameter for the P2MP instance is set to the same value as you configured for the parent P2MP LSP.

16 Configure the following parameters in the Administrative Groups panel.

- Inherit Value (for Groups Included)
- Inherit Value (for Groups Excluded)

When you enable the Inherit Value parameters, the Included and/or Excluded Groups for the P2MP instance are set to the same values you configure for the parent P2MP LSP. If you do not enable the Inherit Value parameters, you can configure the Included Groups and Excluded Groups for the P2MP Instance independently from the parent P2MP LSP. (See step 21.)

17 Click on the S2L Paths tab.

18 Click the Create button. The S2L Path (Create) form opens. Each S2L Path object represents a root-to-leaf (S2L) sub-LSP path for the primary instance of the P2MP LSP.

19 Configure the parameters.

- Name
- ID
- Destination Site ID
- Administrative

20 Repeat steps 18 and 19 to configure another S2L Path, if required.

21 Click on the Administrative Groups tab.

22 Assign one or more MPLS administrative groups to the P2MP Instance.

- **i** Choose the required Included Groups in the Unassigned list.
- **ii** Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.
- **iii** Select the required Excluded Groups in the Unassigned list.
- **iv** Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

  After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the P2MP Instance Properties tab.

23 Click on the OK button. The P2MP Instance (Create) form closes.

24 Click on the S2L Paths tab in the main P2MP LSP (Create) form.

25 Click on the Search button to populate the table. The S2L Paths you configured in step 18 appears. You can select an entry from the list and click on Properties to edit it, if required.

26 Click on the Administrative Groups tab in the main P2MP LSP (Create) form.

27 Assign one or more MPLS administrative groups to the P2MP LSP.

- **i** Select the required Included Groups in the Unassigned list.
- **ii** Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.
- **iii** Select the required Excluded Groups in the Unassigned list.
- **iv** Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.

  After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmap) and Groups Excluded (bitmap) indicators on the P2MP LSP Properties tab.

28 Click OK to close the P2MP LSP (Create) form.

29 Close the Manage Point-to-Multipoint LSPs form.

30 To complete the configuration of the Point-to-Multipoint LSP, you must:

- **a** Configure the required PIM tunnel interfaces. See Procedure 30-2.
- **b** Configure tunnel interfaces on the required IGMP routing instance. See Procedure 31-37.
- **c** Configure tunnel interfaces on the required multicast info policy. See Procedure 49-4 for more information.

31 After you complete the configuration of the Point-to-Multipoint LSP, you can reopen the P2MP LSP form to create, configure and run OAM diagnostics, if required.

- **i** Click on the Tests tab button. The Test Suite, P2MP Ping, and P2MP Trace tabs are displayed.
- **ii** Create or search for the test suite or particular type of test you want to run from the tab pages. Click on either the Create or Search buttons as required.
- **iii** Click the Execute button to run a selected test.

  Refer to chapters 38 and 78 for more information about configuring OAM diagnostics.

Procedure 32-15 To create a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form appears.

2 Click on the Create button. The Create Bypass-only LSP form opens with the Identification step displayed.

3 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the manual bypass LSP.

Note — You can also manually specify an IP address for each parameter in this step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

ii Select a site in the list and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the source site information, which includes the Source IP Address parameter value. This parameter is automatically populated with the system IP address of the site.

iii Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

iv Select a site in the list and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path form opens.

7 Configure the Auto Select Hop-less Path parameter.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The LSP-Path Binding opens, with the Choose MPLS Path step displayed.

i Select an MPLS path in the list to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 32-4 for more information.

ii Click on the Next button. The Set Traffic Options step is displayed.

iii Configure the parameters.

- Hop Limit
- Inherit Value
- Record Actual Path

iv Click on the Next button. The Set Initial States step is displayed.

v Configure the Administrative parameter.

vi Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

vii Click on the OK button. The Create Bypass-only LSP form reappears.

10 Click on the Next button. The Properties step is displayed.

11 Configure the Hop Limit parameter in the Traffic Engineering And Protection block.

12 Configure the Make before Break parameter.

13 In the CSPF block, configure the parameters:

- Enable CSPF
- TE Metric
- Inter Area CSPF To First Loose Hop

14 Configure the following parameters in the Signalling block:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

15 Configure the following parameters in the Inter Area/Level Traffic Engineering block:

- Exclude Node in ERO
- Exclude Node IP Address

16 Click on the Next button. The Admin Groups step is displayed.

17 Assign one or more included MPLS administrative groups to the bypass-only LSP.

i Select the required MPLS administrative groups in the Included Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.

Note — When you assign included administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Included (bitmask) indicator on the General tab.

18 Assign one or more excluded MPLS administrative groups to the bypass-only LSP, if required.

i Select the required MPLS administrative groups in the Excluded Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.

Note — When you assign excluded administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Excluded (bitmask) indicator on the General tab.

19 Configure the Propagate Admin Group parameter.

20 Click on the Next button. The Set Initial State step is displayed.

21 Configure the Administrative parameter.

22 Click on the Finish button. The 5620 SAM prompts you to view the bypass-only LSP.

23 Enable the View the newly created Bypass Only Lsp parameter to view the bypass-only LSP configuration after closing the form, if required.

24 Click on the Close button. The Create Bypass-only LSP form closes.

25 If the View the newly created Bypass Only Lsp parameter in step 23 is enabled, the Bypass-only LSP (Edit) form opens with the newly created bypass-only LSP configuration displayed.

  i View the configuration, if required.

  ii Close the Bypass-only LSP (Edit) form.

26 Close the Manage Manual Bypass LSPs form.

Procedure 32-16 To view and configure a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of Bypass-only LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Bypass-only LSP (Edit) form opens with the General tab displayed.

4 Click on the desired tab buttons to view or configure information about the bypass-only LSP, as required.

5 If you have made any configuration changes, click on Apply or OK in the Bypass-only LSP (Edit) form and a dialog box appears.

6 Click on the Yes button. The Bypass-only LSP (Edit) form closes.

7 Close the Manage Manual Bypass LSPs form.

Procedure 32-17 To configure an LSP path

The following procedure applies to Dynamic LSPs and Manual Bypass LSPs, unless otherwise noted. Dynamic LSPs are used to demonstrate the steps.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of dynamic LSPs is displayed.

3 Select a dynamic LSP from the list.

4 Click the on Properties button. The Dynamic LSP (Edit) window opens with the General tab displayed.

5 Click on the LSP-Path Bindings tab button. A list of LSP paths is displayed.

6 If you are accessing this form to update the MPLS path for a Dynamic LSP, then go to step 10. Otherwise, go to step 7.

7 Select an LSP-Path Binding from the list and click on the Properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

8 Configure the parameters:

- Type
- Administrative
- Backup Type
- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Record Label
- Diff-Serv Class Type
- Inherit Value
- Diff-Serv Backup Class Type
- Make before Break
- Inherit Value
- Resignal
- Enable CSPF
- Groups Included
- Inherit Value
- Groups Excluded (bitmap)
- Inherit Value

The Diff-Serv Backup Class Type parameter is only applicable to Dynamic LSPs.

9 Replace the existing MPLS path for a primary or secondary LSP with another MPLS path, if required, by proceeding as follows:

Note — You can update the existing MPLS path only for a primary or secondary LSP path that has the Make before Break parameter enabled, and that has a release 8.0 or later source NE. The MPLS path you want to use must already exist on the NE, and must not be used by any other LSP paths under the parent LSP.

i Click on the More Actions button and choose Update MPLS Path. The Choose MPLS Path form opens and displays the eligible MPLS paths.

ii Select the required MPLS path from the list.

iii Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding (Edit) form is refreshed with the parameters related to the updated MPLS path selection.

iv Click on the OK button. The The LSP-Path Binding (Edit) form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

v Go to step 14.

10 Select the MPLS path from the list that you want to use to replace the existing path. Refer to the Note in step 9 for restrictions.

11 Click on the More Actions button and choose Update MPLS Path. The Choose MPLS Path form opens and displays the eligible MPLS paths.

12 Select the required MPLS path from the list.

13 Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

14 Click the Set as Secondary or Set as Standby buttons for a selected LSP-Path Binding to change its Type to one of these choices, if required.

15 Click the Switch Standby to Standby button for a selected LSP-Path Binding if you need to switch from the current active standby LSP path to another standby LSP path. This applies only to dynamic LSPs. The button choices include:

- Switch: This option allows you to switch manually from an active standby path to another inactive standby path. You can do this as often as required, without having to select Clear first.
- Force Switch: This option is essentially the same as the Switch option, but you cannot switch back unless you first press Clear to remove the Force Switch flag.
- Clear: This option is used to clear the Force Switch flag.

16 Click on the Administrative Groups tab button.

17 Assign an MPLS administrative group to the dynamic LSP.

i Select an MPLS administrative group in the Unassigned list.

ii Click on the right arrow button. The group is assigned to the dynamic LSP and moves to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the assigned groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

18 Click on the General Tab and in the Shared Risk Link Group panel, configure the Enable SRLG for FRR or Enable SRLG parameter, if available and required.

19 Click on the Tests tab button to configure OAM diagnostics for the LSP path, if required. The supported test type tab buttons appear. See chapter 38 for more information about configuring OAM diagnostics.

20 View a list of hops, if required.

i Click on the following tab buttons to list the path hops, if required:

- Provisioned Path
- Actual Path
- CSPF Path

ii Click on the Topology View button to view the topology map for the path, if required. See chapter 5 for information about using topology maps.

21 Click on the OK button. The LSP-Path Binding (Edit) form closes.

22 Click on the OK button. The Dynamic LSP (Edit) form closes.

Procedure 32-18 To create an LSP path using a tunnel template

Before you can create an LSP path from a tunnel template, you must create the tunnel template. You can use an existing LSP path to create a tunnel template. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs window opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template form opens with a list of previously created templates.

3 Choose a LSP template from the list. The template must be one where you associated a child LSP Path template to the parent LSP template. See Procedure 6-3 for information about creating parent and child objects for tunnel templates.

4 Click on the OK button. A Create Dynamic LSP from Template window opens. See Procedure 32-9 for information about creating a dynamic LSP from a template.

5 Click on the OK button. The Dynamic LSP (Edit) form opens.

6 Click on the LSP-Path Bindings tab button.

7 Click on the Create from Template button. A pop-up menu appears with an LSP path template.

8 Click on the template that you want to use for the LSP path.

9 Configure the parameters:

- Type
- Administrative
- Fast Reroute
- Backup Type
- Hop Limit
- Backup Setup Priority
- Backup Hold Priority
- Minimum Bandwidth (mbps)
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Reserved Bandwidth
- Hop Limit
- Record Actual Path
- Record Label
- Persistent
- Permit Merge
- IGP Shortcut Enabled
- Diff-Serv Class Type
- Diff-Serv Backup Class Type
- Main Class Type Retry Limit
- Make before Break
- Resignal
- Enable CSPF
- Rebuild Timer
- Groups Included
- Groups Excluded (bitmap)
- Groups Included
- Enable SRLG
- Show created object

The IGP Shortcut Enabled, Diff-Serv Backup Class Type, and Main Class Type Retry Limit parameters are configurable for LSPs that have source NEs at Release 8.0 or later.

10 Click on the Inheritance tab button.

11 Configure the Overridden Properties parameter.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Create LSP Path From Template form closes.

14 Close the Manage Dynamic LSPs window.

Procedure 32-19 To configure an LSP Path optimization policy

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Click on the Create button. A drop-down menu appears.

4 Choose Create Optimization Policy. The LSP Path Optimization Policy (Create) window opens with the General tab displayed.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Description

6 Click on the Candidate Definition tab button to apply filters to define eligible LSP Paths for optimization. When no filters are applied, all eligible LSP Paths are listed in the Execution Candidates window.

7 To further limit the number LSP Paths that are listed in the Execution Candidate window, define rule-based groups and add only those NEs that contain the LSP Paths that you need include.

   i Click on Select button beside the Filter Name parameter in the LSP Path Filter panel. A Select LSP Path Filter dialog box appears.

   ii Apply a filter, or create and apply a filter and click on the Search button. A list of LSP Path filters is displayed.

   iii Choose an LSP Path filter from the list.

   iv Click on the OK button. The LSP Path Filter panel is refreshed with the selected LSP Path Filter.

   v Click on Select button beside the Filter Name parameter in the Dynamic LSP Filter panel.

   vi Apply a filter, or create and apply a filter and click on the Search button. A list of dynamic LSP filters is displayed.

   vii Choose a dynamic LSP filter from the list

   viii Click on the OK button. The Dynamic LSP Filter panel is refreshed with the selected dynamic LSP filter.

   ix Click on Select button beside the Name parameter in the Rule-Based Group panel. A list of rule-based groups is displayed

   x Choose a rule-based group from the list.

   xi Click on the OK button. The Rule-Based Group panel is refreshed with the selected rule-based group.

8 Click on the Execution Rules tab button. Configure the parameters:

- Sequencing Target
- Sequencing Order
- Pacing Interval (seconds)

9 Click on the Apply button, the window is refreshed with schedule information.

Note 1 — The Schedule Optimization button does not appear during LSP path optimization policy creation. The LSP path optimization policy must be created first before a schedule can be applied. You must click on the Apply button.

Note 2 — After a schedule is applied to a LSP Optimization Policy, you cannot make changes to the schedule from the Optimization Scheduled Task window.

10 Click on the Schedule Optimization button. An Optimization Scheduled Task (Create) form opens.

11 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

12 Click on the Select button beside the ID parameter. A Select Schedule - Optimization Scheduled Task window opens.

13 Perform one of the following:

a Click on the Create button to create a schedule. A SAM Schedule Create form opens. See Procedure 79-1 for more information about creating a schedule.

b Choose a previously created schedule.

14 Click on the OK button. The Optimization Scheduled Task window refreshes with the schedule and optimization information.

15 Click on the OK button. The Select Schedule - Optimization Scheduled Task window closes and the LSP Path Optimization Policy window reappears.

16 Click on the Execution Candidates tab button.

17 Click on the Search button to display only the eligible LSP Paths that were filtered in step 7. If a filter was not applied, all eligible LSP Paths are listed.

18 Click on the Optimize button. To view the results of optimization, see Procedure 32-21.

19 Close the LSP Path Optimization Policy window.

Procedure 32-20 To terminate an LSP Path optimization policy that is in progress

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Create a filter to search for optimization policies that are in progress. Click on the Search button. A list of LSP Path optimization policies that are in progress appears.

4 Choose a LSP Path optimization policy from the list.

5 Click on the Properties button. The LSP Path Optimization Policy (Edit) window opens with the General tab displayed.

6 Click on the More Actions button and choose Stop Current Optimization. The Optimization parameter value changes from In Progress to Not In Progress.

7 Close the LSP Path Optimization Policy (Edit) window.

Procedure 32-21 To view LSP Path optimization policy results

Use the following procedure to view the re-signaling information as a result of the LSP Path optimization policy execution. See Procedure 32-19 for more information about configuring a LSP Path optimization policy.

1 Choose Manage→MLPS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Select LSP Path (Path/Routing Management MPLS) from the drop-down menu.

3 Click on the Search button. A list of LSP Paths appears.

4 Choose the LSP Path on which you executed a LSP optimization policy.

5 Click on the Properties button. An LSP-Path Binding (Edit) window opens.

6 View the following parameters, as described in section 32.1.

- Resignal Eligible
- Last Performed Type
- Last Performed
- Last Performed State

7 Close the LSP-Path Binding window.

8 Close the Manage LSP Path Optimization window.

Procedure 32-22 To view detour and bypass path information

Perform this procedure to view information regarding detour and bypass tunnel paths and their protected LSPs. Detour and bypass paths are typically configured for fast-reroute-enabled LSPs on NEs for service protection against NE or link failure. The RSVP protocol is used to detect an NE or link loss.

Note 1 — This procedure applies to dynamic LSPs only.

Note 2 — Detours are employed in One-to-One backup configurations. A separate backup LSP is established for each LSP that is backed up.

Bypass Tunnels are employed in Many-to-One backup configurations in which a single backup LSP is used to back up multiple original LSPs.

Whether a path is a detour or bypass path is determined by the Backup Type value specified during LSP creation. The Backup Type parameter can be set only when Fast Reroute for the LSP is set to true.

1 Navigate to a dynamic LSP that you want to examine. The path is Manage→MPLS→Dynamic LSPs.

2 Select the required LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

3 Click on the RSVP Sessions tab button. The detour or bypass originating, transiting, and terminating RSVP sessions associated with the LSP are listed. Type, site, next and previous hop, and other related information is available.

4 Select the desired RSVP session of type detour or bypass from the list and click on the Properties button. The Session (View) form opens.

5 To view the Protected LSPs for the specific bypass or detour:

- **i** Click on the Protected LSP Paths tab button. All the protected LSPs for a specific bypass or detour tunnel are listed.
- **ii** Use the scroll bar at the bottom of the list frame to view the available information on the Protected LSPs.

6 To view the Detour or Bypass Tunnel Paths for the detour or bypass tunnel:

- **i** Click on the Detour/Bypass Tunnel Path tab button. Information regarding the detour or bypass paths is displayed. Sufficient information is provided to permit tracing a path from its originating site, through its transit hops, and to its termination site.
- **ii** Use the scroll bar at the bottom of the list frame to view the available information on the paths, including ID, Type, and so on.

7 To view additional specific Detour or Bypass information, perform the following steps, as appropriate:

- **a** For a selected detour session, click on the Detour tab button. The Detour Session ID, Detour PLR ID, and Avoided Downstream Site ID are listed.
- **b** For a selected bypass session, click on the Bypass Tunnel tab button. The Bypass Tunnel's current State is displayed.

Note — For 5620 SAM to accurately gather the information about the detour and bypass tunnel path (and the LSPs protected by a detour or a bypass tunnel), 5620 SAM must be managing all routers participating the LSP fast reroute. This is required by 5620 SAM for all SR and 7705 SAR nodes along the primary path of a fast reroute-enabled LSP.

Procedure 32-23 To create an LSP template for MVPN

1 Choose Policies→MPLS→LSP Template MVPN from the 5620 SAM main menu. The Manage LSP Template for Mvpn form opens.

2 Perform one of the following:

- **a** Configure the Policy scope parameter to Global.
- **b** Configure the Policy scope parameter to Local.
  - **i** Configure the Local Node IP Address parameter, if required
  - **ii** Click on the Select button and choose a device.

3 Click on the Create button. The LSP Template MVPN Policy (Create) form opens.

4 Configure the parameters:

- Displayed Name
- Description

5 Click on the Properties tab button.

6 Configure the parameters in the Traffic Engineering and Protection panel:

- Reserved Bandwidth
- Fast Reroute
- Hop Limit
- Record Actual Path
- Record Label

7 Configure the parameters in the Fast Reroute panel:

- Backup Type
- Hop Limit

Note — The Backup Type and Hop Limit parameters are configurable if the Fast Reroute parameter is set to true.

8 Configure the Make before Break parameter.

9 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

10 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit

11 Click on the Administrative Groups tab button.

12 Assign one or more MPLS administrative groups to the LSP template MVPN policy.

i Choose the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

iii Choose the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the LSP Template MVPN Policy Properties tab.

13 Click on the OK button. The LSP Template MVPN Policy, Global Policy (Create) form closes and the Manage Lsp Template for Mvpn form reappears with the LSP MVPN template displayed.

14 Choose the LSP MVPN template and click on the Properties button. The LSP Template MVPN Policy - Global Policy (Edit) form opens with the General tab displayed.

15 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when the policies are used by resources on the device.

Note 1 — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

Note 2 — The MVPN LSP template cannot be used until you choose a default MPLS path and configure the Administrative parameter in the local policy definition after the global policy is distributed. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes are saved.

16 Click on the Local Definitions tab button.

17 Click on the Search button. A list of LSP MVPN templates is displayed.

18 Choose an LSP MVPN template from the list and click on the Properties button. The LSP Template MVPN Policy, Local Policy (Edit) form opens with the General tab button displayed.

19 Click on the Switch Mode button to change the configuration mode to Local Edit Only.

20 Click on the Properties tab button.

21 Click on the Select button to choose a default MPLS path. The Select Default MPLS Path - Lsp MVPN Template, Local Policy window opens with a list of default MPLS paths displayed.

22 Choose an MPLS path from the list and click on the OK button. The default MPLS path is displayed.

23 Click on the General tab button.

24 Configure the Administrative parameter.

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The LSP Template MVPN Policy, Local Policy form closes.

Procedure 32-24 To list and view MPLS objects

1 Choose Manage→MPLS→MPLS Objects from the 5620 SAM main menu. The Manage MPLS Objects form opens.

2 Select an MPLS object type in the list and click on the Search button. A list of MPLS objects is displayed.

3 Select an object in the list and click on the Properties button. The properties form for the object appears.

4 View the information on the various tabs, as required.

5 Close the object properties form.

6 Close the Manage MPLS Objects form.

33 — Service tunnels

33.1 Service tunnel overview

A service tunnel is an entity used to uni-directionally direct traffic from one device to another device. The service tunnel is provisioned to use a specific encapsulation method, such as GRE or MPLS, and the services are then mapped to the service tunnel. For instance, multi-node VLL and VPLS traffic is transmitted using uni-directional service tunnels in this way.

The most common type of tunnel used in 5620 SAM is a Service Distribution Point binding. Service tunnels originate on an SDP on a source NE and terminate at a destination NE. The destination NE directs packets from the service tunnel to the correct service egress interfaces (SAPs) on that device. Services that originate and terminate on the same NE do not require service tunnels, since the same NE is both the source and the destination.

However, since the concept of a tunnel is a logical construct within 5620 SAM, a number of different configurable objects can actually be used as service tunnels, including:

- SDP binding:
  Since SDP bindings can be associated to a service of any type, the service tunnel discovery includes services that are associated to SDP bindings of a given service.
- Service to Tunnel Association:
  Discovery adds tunnels that are associated to a given service.
- Ethernet tunnel (G.8031):
  Discovery adds the global Ethernet Tunnel that the Tunnel Endpoint (SAP's terminating port) is a member of.
- Ethernet ring (G.8032):
  Discovery adds the Ethernet Ring that the Ethernet Element is a member of.
- Ethernet radio ring (G.8032):
  Discovery adds the Ethernet radio ring that the Ethernet Element is a member of.
- PBB:
  Discovery adds the VPLS or MVPLS services which contain the PBB tunnel (B-Sites) of the given Epipe or VPLS.
- P2MP RSVP LSP:
  Discovery adds the P2MP LSPs retrieved from the MVPN LSP Template associated to PIM sites.
- Optical Transport Service:
  Discovery adds optical services that are traversing through network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service.
- Mobile backhaul (applicable to 9500 MPR and 7705 SAR on MPLS-based services running over VLAN):
  Discovery adds MPR VLL services that are either associated to an SDP tunnel or are traversing through network interfaces which are being used by an L2/L3 VPN through any static or dynamic LSPs that are bound to SDPs on the service.

The Service Tunnels tab exists on all applicable service configuration forms. This tab lists all objects considered as service tunnels (SDPs, Ethernet rings, Ethernet tunnels, other services, and so forth) that are currently used by the service you are querying. The associated Discover Service Tunnels button removes any previously discovered service tunnels on the service and triggers a manual re-discovery of these, based on direct usage and current service configurations.

For composite services, the service tunnel discovery action triggers the discovery of service tunnels on all participating services. Hence, the listing includes all service tunnels currently being used by member services.

Another tab titled Flow-through Services also exists on the configuration forms of all the objects that can be used as a service tunnel. This tab lists all other services that are currently using the object you are querying as a service tunnel. The associated Discover Flow-through Services button removes any previously discovered flow-through services and triggers a manual re-discovery of these, based on direct usage and current service configurations.

For composite services, the concept of using a service as a service tunnel is not currently supported. Therefore, the Flow-through Services tab does not appear on the composite service configuration forms.

For fault management, note that an “association” type of alarm relationship exists between a service and the service tunnels it uses. This allows the service tunnel alarms to propagate up to the service level. These association alarms are displayed on the Alarms on Related Objects sub-tab, under the Faults tab of the service. Since this is a one-way association relationship, no service alarms are propagated to the service tunnels that the service is currently using.

Tunnel selection profiles

A Tunnel Selection Profile is used by 5620 SAM to assign transport tunnels for a service when the service has been configured for automatic SDP binding creation. However, for services where the SDP binding creation is performed manually, the Tunnel Selection Profile can also still be used. In these cases, tunnels and return tunnels are chosen by the system when the automatic selection of such transport tunnels is enabled and a Tunnel Selection Profile is specified.

The Tunnel Selection Profile contains Steering Parameters. When the profile is used within a service to create SDP bindings, any tunnels tagged with the Steering Parameters included in that profile become eligible for consideration in the tunnel selection process.

33.2 IP/MPLS service tunnels

Distributed service traffic is transported between PE NEs by circuits aggregated in unidirectional service tunnels.

The operational theory of a service tunnel is that the encapsulation of the data between the two managed edge NEs appears like a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

Tunnel policies from older versions of 5620 SAM can be converted to the newer template-based policies by using a “Convert” button located on the rule configuration form. You cannot configure CoS forwarding, LDP-over-RSVP, or multiple LSP bindings on SDP features.

A service tunnel uses GRE or MPLS encapsulation. For MPLS, a mesh of MPLS paths and LSPs must be present in the network core. You associate service tunnels with LSPs during service tunnel configuration. The 5620 SAM supports LSP creation using a basic LDP variant such as T-LDP, or using LDP over RSVP for tunnel-in-tunnel functionality based on traffic classification.

A 5620 SAM operator binds a service site to a service tunnel during service configuration. A service tunnel has a unique ID on an NE and cannot be deleted when it is currently associated with a service.

ACL IP and ACL MAC policy filters for service tunnels contain options for forwarding packets on a specific service tunnel based on matching criteria, as described in chapter 48.

IP/MPLS service tunnels design considerations

Consider the following before you configure IP/MPLS service tunnels:

- Service tunnels are unidirectional, so they are required in both directions between the source NE and the destination NE.
- The tunnel is not specific to one service or one type of service. After a tunnel exists, multiple SDPs can be aggregated over the tunnel. The SDPs can belong to different services and different customers.
- When a tunnel already exists, 5620 SAM does not automatically create a new tunnel, even if the only available tunnel is down. This prevents the creation of multiple inoperable tunnels.
- All services that are mapped to a tunnel use the same transport encapsulation type defined for the tunnel.
- Operations on the tunnel affect all the services that are associated with the tunnel. For example, the operational and administrative states of a tunnel control the state of service circuits that are carried on the tunnel. In the case of LSP-based tunnels, an LSP can be replaced in the tunnel without reconfiguring each service bound to the tunnel.
- A service tunnel is locally unique to an NE. The same tunnel ID can appear on other NEs.
- A service tunnel uses the system IP address to identify the far-end edge NE.
- A service tunnel can be configured using a tunnel template. A user that is assigned the create tunnel template scope of command role can create a tunnel template. The template manager can also apply the tunnel template to a service tunnel. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with tunnel templates.
- An SDP tunnel template can be applied to an auto tunnel policy.

See the appropriate device documentation for more detailed information about service tunnels.

Class-based forwarding

Packets of the same CoS and service are forwarded over a specific RSVP LSP (or a static LSP), which is part of an SDP that the service (instance) is bound to. The forwarding decision is based on the forwarding class of the packet, as assigned by the ingress QoS policy defined for the SAP.

When implementing class-based forwarding, consider the following:

- Class-based forwarding is typically implemented using the service tunnel configuration forms, as detailed in Procedure 33-1. Class-based forwarding configurations can also be altered after their initial creation by editing the service tunnel configuration form as detailed in Procedure 33-13.
- An LSP can carry packets of a forwarding class for one service and at the same time, carry packets of a different forwarding class for another service. In other words, the same LSP can be used by more than one SDP, even where the forwarding class assignments are different.
- Within an SDP, only one LSP can support a specific CoS.
- A service instance (or service site) can be bound to SDPs of differing CoS configurations, as well as regular SDPs.
- One LSP in the SDP must be designated as the default LSP. The default LSP is used by the SDP if there is no available LSP that matches the packet's forwarding class. When the default LSP is down, the SDP is also brought down.
- Class-based forwarding can be applied to all services supported by the SRs. For VPLS, you can specify an LSP to forward all multicast/broadcast packets (by default, the default LSP is used). For VLL, shared queuing must be enabled on the ingress SAP to support the class-based forwarding.
- Class-based forwarding is configurable on the 7750 SR, 7710 SR, and 7450 ESS

33.3 Ethernet (G.8031) tunnels

The IEEE 802.1ah Provider Backbone Bridging specification employs Provider MSTP to ensure loop avoidance in a resilient native Ethernet core. With P-MSTP, failover times depend largely on the size of the network and the connectivity model used in the network. MPLS tunnels provide core scaling and fast failover times using MPLS FRR. A service based on native Ethernet backbone achieves the same fast failover times as MPLS FRR.

Core Ethernet tunnels compliant with the ITU-T G.8031 specification achieve 50 ms resiliency for backbone failures. A configured Ethernet tunnel can be selected when configuring an L2 access interface on a B-VPLS.

The 5620 SAM uses two different approaches to configure Ethernet tunnels in the network.

- Approach 1 (recommended):
  5620 SAM provisions an end-to-end Ethernet G.8031 tunnel which reduces configuration errors and aids the diagnosis of any problem in the tunnel. 5620 SAM automatically configures the Ethernet tunnel endpoint and path endpoint on each of the participating NEs. See Procedure 33-6 for more information.
  The Ethernet tunnel and path are network wide objects that provide the following benefits:
  - the Ethernet tunnel provides the aggregated State of the Tunnel and reports any inconsistency in the configuration of the endpoints or paths
  - faster and easier provisioning that allows you to configure common properties such as holdTime and revertTime at the network level and then apply them to each tunnel endpoint
  - 5620 SAM accelerates the creation of global and local MAs, and MEPs by using a continuity check
- Approach 2:
  The 5620 SAM provides the ability to provision Ethernet tunnel endpoints and path endpoints separately on each NE. See Procedure 33-5 for more information on creating Ethernet endpoints. If Ethernet tunnel endpoints are created this way (or discovered from the NE) you can associate them to a network-wide Ethernet tunnel and path, but this must be done manually.

Note — Network-wide Ethernet tunnels and paths are not automatically discovered from the NE.

33.4 Ethernet (G.8032) tunnels

Ethernet Ring Protection (ERP) as specified in ITU-T G.8032, is a protection mechanism for Ethernet ring topologies. ERP provides sub-50ms protection and recovery switching for Ethernet traffic in a ring topology, and, at the same time, ensures that loops are not formed at the Ethernet layer. G.8032v1 supports a single ring topology; G.8032v2 supports multiple rings/ladder topology.

ERP topology

An ERP topology is a collection of Ethernet ring nodes that forms a closed physical loop. Between two and sixteen Ethernet ring nodes are supported per ERP topology. One ERP topology is supported per NE. Up to two ERP instances are supported per ERP topology. Ethernet ring links connect two adjacent Ethernet ring nodes participating in the same ERP topology.

Loop avoidance in the ring is achieved by guaranteeing that at anytime, traffic may flow on all but one of the ring links. This link is called the ring protection link (RPL). One designated node, the RPL Owner (also referred to as the master node), is responsible to block traffic over the RPL.

You can configure the following service types in an ERP (G.8032) topology on the following NEs:

- VPLS. VPLS that support ERP SAPs can connect to other rings and Ethernet services using VPLS SAPs.
    - 7210 SAS 3.0, Release 1 or later devices with one exception. ERP is not supported on the 7210 SAS-X 24F 2XFP, Release 3.0 R1. ERP is supported on the 7210 SAS-X 24F 2XFP, Release 3.0 R2.
- VLAN service
    - OS 6400, OS 6850, OS 6850E, OS 6855, OS 9700E, OS 9800E, Release 6.4.4 or later
    - OS 6250M, Release 6.6.2 or later
    - 9500 MPR, Release 3.1 or later
- VLL service (Cpipe and Epipe services only)
    - 9500 MPR, Release 3.1 or later

Note — For OmniSwitch NEs, only the Ethernet ring element configuration (and not Ethernet ring) is supported on the 5620 SAM. See Procedure 33-8 for more information.

33.5 Workflow to configure service tunnels

1 Before you can create a MPLS service tunnel, you must create a static or dynamic LSP. See Procedure 32-6 for statics LSPs. See Procedure 32-8 for dynamic LSPs.

2 As required, create an IP/MPLS service tunnel, an Ethernet service tunnel, or an Ethernet ring and assign it to an NE.

a Create an IP/MPLS service tunnel. See Procedure 33-1 for more information.

b Create an IP/MPLS service tunnel from a tunnel template. See Procedure 33-2 for more information.

c Create an Ethernet service tunnel.

i Create an Ethernet service tunnel endpoint. See Procedure 33-5 for more information.

ii Create an Ethernet service tunnel and assign endpoints to it. See Procedure 33-6 for more information.

d Create an Ethernet ring.

i Create an Ethernet ring element for all supported devices except for OmniSwitch and 9500 MPR devices. See Procedure 33-7 for more information.

ii Create an Ethernet ring element for an OmniSwitch. See Procedure 33-8 for more information.

iii Create an Ethernet radio ring element for an 9500 MPR. See Procedure 33-9 for more information.

iv Create an Ethernet ring and assign elements to the ring. See Procedure 33-10 for more information.

Note — Service tunnels are unidirectional, so they are required in both directions between the source NE and the destination NE.

3 If you created an IP/MPLS service tunnel in step 2, create a steering parameter and a tunnel selection profile and assign the tunnel selection profile to an SDP binding.

i Create a steering parameter. See Procedure 33-3 for more information.

ii Create a tunnel selection profile. See Procedure 33-4 for more information.

33.6 Configuring service tunnel procedures

Procedure 33-1 describes how to create an IP/MPLS service tunnel.

Procedure 33-1 To create an IP/MPLS service tunnel

Before you can create a MPLS service tunnel, you must create a static or dynamic LSP. See Procedure 32-6 for statics LSPs. See Procedure 32-8 for dynamic LSPs.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose IP/MPLS Service Tunnel (SDP). The IP/MPLS Service Tunnel (SDP) step form opens with the Name & Describe Service Tunnel (SDP) step displayed.

3 Configure the parameters.

- Name
- Description
- Auto-Assign ID
- ID

Note 1 — If a range policy is applied to a service tunnel, a grey text box appears beside the ID parameter to indicate that a range policy is in effect.

Note 2 — If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation to indicate that a format policy is in effect. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to choose a policy. The sequence of the options in the combo box are ordered by the policy Priority parameter.

4 Click on the Next button. The Pick Source Node step is displayed.

5 Configure the Source Site ID parameter. Perform one of the following:

  a Choose an NE from the list.

    i Click on the Select button. The Select a Network Element - Pick Source Node form opens.

    ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Source Node form closes and the Create Service Tunnel (SDP) form displays the source NE IP address.

  b Enter the NE IP address.

6 Click on the Next button. The Pick Destination Node step is displayed.

7 Configure the Destination Site ID parameter. Perform one of the following:

  a Choose an NE from the list.

    i Click on the Select button. The Select a Network Element - Pick Destination Node form opens.

    ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Destination Node form closes and the Create Service Tunnel (SDP) form displays the destination NE IP address.

  b Enter the NE IP address.

8 Click on the Next button. The Specify Transport step is displayed.

9 Perform one of the following:

a For GRE service tunnels:

i Specify GRE for the Underlying Transport parameter.

ii Configure the Signaling parameter.

iii Go to step 19.

b For MPLS service tunnels:

i Specify MPLS for the Underlying Transport parameter.

Note 1 — If the source or destination site is a 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7250 SAS-ES, you cannot configure the Underlying Transport parameter. The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7250 SAS-ES support only MPLS with TLDP signalling, LDP is not enabled.

Note 2 — When you implement class-based forwarding or specify a transport destination address, you must select MPLS as the Underlying Transport parameter.

Note 3 — When you specify a transport destination address, you cannot implement class-based forwarding.

Note 4 — When you configure a service tunnel whose source site is a 7705 SAR (version 3.0 or later), you may select IPv4 as the Underlying Transport parameter if the destination site is also a 7705 SAR (version 3.0 or later), a GNE, or an unmanaged IP address.

ii Configure the parameters:

- Mixed Lsp Mode
- Revert Time (seconds)
- Ldp Enabled
- Bgp Tunnel Enabled
- Signaling

The Revert Time (seconds) parameter displays when the Mixed Lsp Mode parameter is set to true.

Note 1 — When you implement class-based forwarding, you must use one of the following parameter configurations:

- Set Mixed Lsp Mode to true.
- Set Mixed Lsp Mode, Ldp Enabled, and Bgp Tunnel Enabled parameters to false.

Note 2 — When you specify a transport destination address, you must use the following parameter configurations:

- Set Ldp Enabled to true.
- Set Mixed Lsp Mode and Bgp Tunnel Enabled to false.

Note 3 — You cannot set Bgp Tunnel Enabled to true when Ldp Enabled or Mixed Lsp Mode is set to true.

Note 4 — You cannot create a BGP or an LDP tunnel when an LSP exists between the source and destination nodes you chose in steps 4 and 7 respectively.

iii If you set the Ldp Enabled parameter to true, go to step 17.

iv If you set the Bgp Tunnel Enabled parameter to true, go to step 19.

10 Click on the Next button. The Specify Class Forwarding step is displayed.

11 Configure the parameters:

- Class Forwarding Capability
- Administrative State
- Enforce Diff-Serv Lsp-Fc Map

Note — When the Class Forwarding Capability parameter is set to Off, the existing class-forwarding configurations are removed.

The Administrative State and Enforce Diff-Serv Lsp-Fc Map parameters are configurable when the Class Forwarding Capability parameter is set to On.

12 Click on the Next button. The Associate LSPs step is displayed.

13 Click on the Add button to bind an LSP to the service tunnel. The Bind LSPs to Service Tunnel form opens with the Bind LSP to Service Tunnel Stage step displayed.

14 Select an LSP and click on the Finish button.

15 Click on the Close button. The Bind LSPs to Service Tunnel form closes and the LSP is listed on the Create Service Tunnel (SDP) form.

16 If you are enabling class-based forwarding on the LSP:

a Select an LSP from the list and click on the Set As Default LSP button. This is mandatory. The Default LSP Name appears in the associated field.

b For a VPLS, you can optionally specify an LSP to forward all multicast/broadcast packets. If this is not specified, the default LSP is used. If it is specified, the Multicast LSP Name appears in the associated field.

c For any LSPs used for class-based forwarding (including the default), you must select the LSP from the list and click on the Choose a Forwarding Class button. Select the desired forwarding class from the fly-out menu. Your choice appears in the Forwarding Class to LSP Mappings table.

d When you have finished configuring the LSPs, go to step 17. If the source is a 7250 SAS-ES site, go to step 27.

17 Click on the Next button. The Specify Transport Destination Address step is displayed.

Note — This step displays if the Underlying Transport parameter you specified in step 9 was set to MPLS and the Ldp Enabled parameter was set to true.

18 Configure the Transport Destination Address parameter.

19 Click on the Next button. The Specify Hello Parameters step is displayed.

20 Configure the parameters.

- Keep-Alive Enabled
- Hello Time
- Hello Request Timeout
- Max Drop Count
- Hello Message Length
- Hold Down Time

21 Click on the Next button. The Specify MTU Values step is displayed.

22 Configure the parameters.

- Administrative MTU
- Advertised MTU Override

23 Click on the Next button. The Specify Metric step is displayed, if applicable.

24 Configure the Metric parameter, if applicable.

25 Click on the Next button. The VC Type Related Parameters step is displayed, if applicable.

26 Configure the VLAN VC Ethertype parameters, if applicable.

27 Click on the Next button. The Specify Initial State step is displayed.

28 Configure the Administrative parameter.

29 Click on the Next button. The Booking Factor step is displayed.

Note — This step displays if the Underlying Transport parameter you specified in step 9 was set to MPLS and the Ldp Enabled parameter was set to false.

30 Configure the SDP Bandwidth Booking Factor (%) parameter.

31 Click on the Next button. The Associate Service step is displayed.

32 Click on the Select button. The Select Associated Service window opens.

33 Choose a service from the list and click on the OK button. The Select Associated Service window closes. The Associated Service Name and Associated Service ID are updated.

34 Click on the Next button. The Steering Parameters step is displayed.

35 Select the Steering Parameters in the Unassigned list that you want to assign to the tunnel and click the right-pointing arrow to move them into the Assigned list.

36 Click on the Next button. The Network Domain step is displayed.

37 Click the Select button. The Select Network Domain window opens.

38 Choose a network domain from the list and click on the OK button. The Select Network Domain window closes. The Name field is updated.

Note — All SDPs are associated with a network domain. This association is done during the creation or when editing an SDP in the Tunnel (Edit) form. You can also modify the network domain in the Tunnel (Edit) form. See step 42. The Egress Interfaces Consistency State status specifies if all the interface associations to SDP belong to a particular domain.

39 Click on the Finish button to save the configuration. The 5620 SAM prompts you to view the service tunnel configuration.

40 Enable the View the newly created tunnel parameter to view the service tunnel configuration after closing the form, if required.

41 Click on the Close button. The Create Service Tunnel (SDP) form closes.

42 If the View the newly created tunnel parameter in step 40 is enabled, the Tunnel (Edit) form opens with the newly-created service tunnel configuration displayed.

- **i** View or modify the configuration, if required.
- **ii** Click on the Create a template button, if required. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.
- **iii** Close the Tunnel (Edit) form.

43 Close the Manage Service Tunnels form.

Procedure 33-2 To create an SDP using a tunnel template

Before you can create an SDP from a tunnel template, you must create the SDP tunnel template. For more information about creating SDP tunnel templates, see the *5620 SAM Scripts and Templates Developer Guide*.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create from Template button. A Create Service Tunnel From Template window opens with a list of previously configured SDP tunnel templates.

3 Choose a tunnel template from the list.

4 Click on the OK button. A Create Tunnel from Template form opens with the General tab displayed.

5 Configure the parameters.

- Name
- Description
- Auto-Assign ID
- ID
- Underlying Transport
- PBB Ethernet Type
- Ldp Enabled
- Signaling
- Source Site ID
- Destination Site ID
- Transport Destination Address
- Administrative
- Administrative MTU
- Advertised MTU Override
- Metric
- VLAN VC Ethertype
- No VLAN VC Ethertype

6 Click on the SDP Bandwidth tab button. Configure the SDP Bandwidth Booking Factor (%) parameter.

7 Click on the Maintenance Tab button and configure the following parameters:

- Keep-Alive Enabled
- Hello Time
- Hello Message Length
- Hello Request Timeout
- Hold Down Time
- Max Drop Count

8 Click on the Accounting tab button.

9 Click on the Select button beside the Accounting Policy parameter to assign an accounting policy to the service tunnel. A Select Policy window opens with a list of accounting policies.

10 Choose a policy from the list and click on the OK button. The Select Policy widow closes and the Accounting Policy parameter is updated

11 Configure the Show created object parameter, if required.

12 Click on the OK button. When the SDP configuration is successful, the Create SDP from Template form closes and the Tunnel (Edit) form appears.

If the SDP configuration is unsuccessful, the Create SDP from Template form remains open and an error message appears.

13 Close the Tunnel (Edit) form.

Procedure 33-3 To create a Steering Parameter

A Steering Parameter is assigned to a service tunnel and acts as a marker for the Tunnel Selection Profile. More than one Steering Parameter can be assigned to a tunnel.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose Steering Parameter. The Steering Parameter (Create) form opens.

3 Configure the Name and Value parameters.

4 Click on the OK button. The Steering Parameter (Create) form closes.

Note — You can also examine an existing Steering Parameter by conducting a search using the Manage Service Tunnels form. Viewing an existing Steering Parameter displays Service Tunnels and Tunnel Selection Profiles tab pages. These allow you to see which of these items make use of the Steering Parameter. A Faults tab displays any related alarms that have been logged.

5 Close the Manage Service Tunnels form.

Procedure 33-4 To create a Tunnel Selection Profile

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose Tunnel Selection Profile. The Tunnel Selection Profile (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Profile Name
- Description
- Transport Type
- Multi-Segment Tunnel Selection
- Redundant Path Selection

4 Click on the Select button.

5 Choose an SDP Binding Template from the list, if required, and click OK. The Script ID, Name, and Description fields for the selected SDP Binding Template are populated in the Tunnel Selection Profile (Create) form.

Note — Specifying an SDP Binding Template in the profile allows the 5620 SAM to use the configuration information contained in the template for the automatic creation of SDP bindings. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.

6 Click on the Steering Parameters tab button.

7 Click on the Steering Parameters that you want to include in the profile in the Included Steering Parameters-Unassigned portion of the form. If you are selecting more than one, hold down the Shift key after your first selection.

8 Click the right-pointing arrow to move the selected Steering Parameters into the Included Steering Parameters-Assigned portion of the form.

You can move an assigned parameter back into the unassigned portion of the form if required, by selecting it and clicking the left-pointing arrow.

9 Click on the Steering Parameters that you want to exclude from the profile in the Excluded Steering Parameters-Unassigned portion of the form. If you are selecting more than one, hold down the Shift key after your first selection.

10 Click the right-pointing arrow to move the selected Steering Parameters into the Excluded Steering Parameters-Assigned portion of the form.

You can move an assigned parameter back into the unassigned portion of the form if required, by selecting it and clicking the left-pointing arrow.

11 Click on the OK button. The Tunnel Selection Profile (Create) form closes.

Note — When configuring an existing profile, the Tunnel Selection Profile (Edit) form displays additional tabs pages, including Services, SDP Bindings, and Spoke Connectors. These allow you to see which of these items make use of the Tunnel Selection Profile. A Faults tab displays any related alarms that have been logged.

12 Close the Manage Service Tunnels form.

Procedure 33-5 To create or configure an Ethernet Tunnel Endpoint

Procedure 33-6 describes how to create a new Ethernet Tunnel Endpoint or configure an existing one.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Tunnel Endpoint, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Tunnel Endpoint from the contextual menu. The Select Network Elements window opens.

5 Choose a site on which to create an Ethernet tunnel endpoint.

6 Click on the OK button. The Ethernet Tunnel Endpoint (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Tunnel Endpoint (Ethernet Tunnel) on the drop-down menu in the Manage Service Tunnels window. Click on the Search button to display a list of the existing endpoints.

9 Select the endpoint you want to configure and click on the Properties button.

The Ethernet Tunnel Endpoint (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- Tunnel Endpoint ID
- Site ID
- Protection Type
- Encap Type
- Administrative State
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Enable Per Forwarding Path Ingress Queue
- Operational Path Endpoint Threshold
- Description
- Configured MAC Address

The Tunnel Endpoint ID and Site ID are only configurable when you are creating a new Ethernet Tunnel Endpoint.

The Access Adapt QoS, Enable Per Forwarding Path Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

11 Click on the Path Endpoints tab button to configure the Path Endpoints.

12 Perform one of the following:

a If you are configuring an existing Ethernet Tunnel Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Tunnel Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Tunnel Path Endpoint, click on the Create button. The Ethernet Tunnel Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Precedence
- APS Command

The Path ID parameter is only configurable when you are creating a new Ethernet Tunnel Path Endpoint.

The APS Command parameter is only displayed and configurable when you are configuring an existing Ethernet Tunnel Path Endpoint and when the Protection Type parameter you configured in step 10 is set to G8031 1:1. The associated “Perform APS Command” button is used to perform the selected command on the path endpoint.

14 Click on the Properties button in the Ethernet Path block if you need to view or alter parameters on the Ethernet Path or configure a CFM Test. The Ethernet Path - Properties button is only displayed and selectable when you are configuring an existing Ethernet Tunnel Path Endpoint.

15 If you are configuring an existing Ethernet Tunnel Path Endpoint, go to step 23.

16 Click on the Port tab.

17 Click on the Select button. The Select Member Port window opens.

18 Click on the Search button to list the available ports. Choose the port to use for the Ethernet tunnel path endpoint.

19 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form displays the selected member port.

20 Configure the parameters:

- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)

21 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form closes and the Path Endpoints tab displays the new Ethernet Tunnel Path Endpoint in the list.

22 Go to step 30.

23 Click on the MEPs tab, if you need to create a MEP for the existing Ethernet Tunnel Path Endpoint. Otherwise go to step 30.

24 Click on the Create button. The MEP (Create) form opens with the General tab displayed.

25 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Control MEP
- Control Sap Tag
- Low-priority Defect
- MAC Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

The Control MEP parameter is only displayed if the Interface Type parameter is set to Ethernet Tunnel Path Endpoint.

The Control Sap Tag parameter is only configurable on a 7210 SAS-M Release 4.0 R2 and later, or a 7210 SAS-X Release 4.0 R2 and later.

Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

26 If the Maintenance Domain for this MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, then the Y.1731 TEST and the AIS tabs will also be displayed. See Procedure 68-18 for more information.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The MEP (Create) form closes and the newly-created MEP is displayed in the list on the MEPs tab.

29 Click on the OK button. The Ethernet Tunnel Path Endpoint (Edit) form closes and the Path Endpoints tab displays the available Ethernet Tunnel Path Endpoints in the list.

30 Repeat steps 12 to 29 for any other Ethernet Tunnel Path Endpoints you need to create or configure.

31 Click OK. A dialog box appears.

32 Click Yes to close the Ethernet Tunnel Endpoint form.

Procedure 33-6 To create an Ethernet tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Tunnel from the contextual menu. The Ethernet Tunnel (Create) window opens.

4 Configure the following parameters:

- Tunnel ID
- Name
- Description
- Protection Type
- Encap Type
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Enable Per Forwarding Path Ingress Queue
- Operational Path Endpoint Threshold

The Access Adapt QoS, Enable Per Forwarding Path Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

5 Click on the Apply button. The Ethernet Tunnel (Edit) window opens with the General tab displayed.

6 Click on the Components tab button. Right click on Tunnel Endpoints and choose one of the following from the contextual menu.

a Create Ethernet Tunnel Endpoint.

i Refer to Procedure 33-5 to create an Ethernet Tunnel Endpoint. The endpoint will be listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.

Note — The parameter values specified in step 4 are automatically applied in the Ethernet Endpoint form when creating an endpoint.

ii Repeat step i to create Endpoint B.

iii Go to step 7.

b Add Existing Endpoint.

i The Select Endpoints window opens.

ii Click on the Search button and select an endpoint.

iii Click OK.

iv The endpoint is listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.

Note — The parameter values specified in step 4 are not automatically applied to the selected Ethernet endpoint.

v Repeat steps i to iv to select Endpoint B.

7 Right click on Paths and choose Create Ethernet Paths from the contextual menu to create a path. The Ethernet Path (Create) window opens with the General tab displayed.

8 Configure the parameters:

- Auto-Assign ID
- ID
- Description

9 Click on the Endpoints tab button. Perform one of the following:

a Manually configure the following parameters for endpoints A and B.

- Site ID
- Path ID
- Precedence
- Administrative State
- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)
- Member Port

Note — A path endpoint cannot be administratively enabled on a Release 8.0 or later NE if either of following is true:

- An operationally up same-fate SAP on the Ethernet tunnel endpoint does not have a tag configured for the path endpoint.
- The Control Tag (Outer Encapsulation Value), Control Tag (Inner Encapsulation Value), and Member Port parameters are not configured.

b Perform the following steps to specify a path endpoint for endpoints A and B.

i Click on the Select button beside the Path ID parameter. The Select Path Endpoint form opens.

ii Click on the Search button and select an available endpoint.

iii Click OK. The endpoint parameters are automatically populated.

Note — To delete an Ethernet tunnel path endpoint, click on the Search button to display a list of endpoints, select an endpoint, then click on the Delete button.

10 Click on the Intermediate Services tab button to view and specify the intermediate services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Create button. The Select Service window opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service window closes and the service you chose is displayed in the list on the Intermediate Services tab.

Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.

Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Create button. The Create button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

11 Click on the CFM Continuity Check tab button to configure a CFM Continuity Check test for each path.

It is mandatory to have the following steps completed before selecting a test:

- Create a Maintenance Domain. The Name Type must be None. See chapter 80 for more information.
- Create a CFM Continuity Check Test. See Procedure 38-6 for information.

12 Click on the Select button. The Select CFM Test window opens.

13 Click on the Search button to list the available CFM tests. Select a CFM test.

14 Click on the OK button. The CFM Test is listed and the MEP Auto Creation check boxes are enabled.

15 Perform one of the following:

a Enable one of the MEP Auto Creation buttons:

i Click on the Run Continuity Check Protocol button to create Maintenance Associations and local and remote MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted. MEPs are turned up and CCM Messages are enabled, and the control MEP property is set on the MEPs.

ii Click on the Create MEPs button to create local MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted.

b Continue to step 16 and select the Run Continuity Check Protocol button or Create MEPs button at a later date.

16 If required, click on the MEP tab button to display the MEP form and select the check box to set the Control MEP parameter.

17 Click on the OK button. The Ethernet Tunnel window is displayed with the new Path information.

18 If the Protection Type parameter in step 4 was set to G8031 1:1, then repeat steps 7 to 17 for the other path.

19 If the Protection Type parameter in step 4 was set to Load Sharing, then repeat steps 7 to 17 for all paths.

20 Click Apply. The Path Id, Operational State, and CC Protocol State are updated and the path endpoints with this specific configuration are sent to the NEs.

> **Note —** The CC protocol state appears under the global path (in the navigation tree and on the CFM Continuity Check form). The CC protocol state displays the state of the continuity check protocol running between the MEPs of the two endpoints of the path.

21 Click OK. A dialog box appears.

22 Click Yes to close the Ethernet Tunnel (Create) form.

Procedure 33-7 To create or configure an Ethernet Ring Element

This procedure describes how to create a new Ethernet Ring Element or configure an existing one.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Ring Element, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Ring Element from the contextual menu.

5 Choose a site from the Select Network Elements window to create an Ethernet Ring Element.

> **Note —** You can create multiple ring elements at this point if you select more than one site here.

6 Click on the OK button. The Ethernet Ring Element (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Ring Element (Ethernet Ring) on the drop-down menu in the Manage Service Tunnels window. Click on the Search button to display a list of the existing ring elements.

9 Select the ring element you want to configure and click on the Properties button.

The Ethernet Ring Element (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Description
- Administrative State
- Compatible Version
- CCM Hold Time Down (deciseconds)
- CCM Hold Time Up (deciseconds)
- Guard Time (deciseconds)
- Revert Time (seconds)
- Ring Protection Link Type
- Ring Node ID

The ID and Site ID are only configurable when you are creating a new Ethernet Ring Element.

11 Configure the parameters for a sub-ring, if required:

- Type
- Ethernet Ring ID
- VPLS
- Propagate Topology Change

12 Click on the Path Endpoints tab button to configure the Path Endpoints.

13 Perform one of the following:

a If you are configuring an existing Ethernet Ring Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Ring Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Ring Path Endpoint, click on the Create button. The Ethernet Ring Path Endpoint (Create) form opens with the General tab displayed.

14 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Path Endpoint Type

The Path ID parameter is only configurable when you are creating a new Ethernet Ring Path Endpoint.

15 If configuring an Ethernet Ring Path Endpoint on a 7210 SAS-M Release 4.0 R2 and later, or a 7210 SAS-X Release 4.0 R2 and later, configure the Switch Command parameter and click on the Perform Switch Command button.

16 If you are configuring an existing Ethernet Ring Path Endpoint, go to step 24.

17 Click on the Port tab.

18 Click on the Select button. The Select Member Port window opens.

19 Click on the Search button to list the available ports. Choose the port to use for the Ethernet ring path endpoint.

20 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form displays the selected member port.

21 Configure the parameters:

- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)

22 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form closes.

The Path Endpoints tab displays the new Ethernet Ring Path Endpoint in the list.

23 Repeat steps 3 to 22 for the other Ethernet Ring Path Endpoint you need to create, if required.

24 Click OK. A dialog box appears.

25 Click Yes to close the Ethernet Ring Element form.

Procedure 33-8 To create or configure an Ethernet Ring Element on an OmniSwitch NE

This procedure describes how to create a new Ethernet Ring Element or configure an existing one on an eligible OmniSwitch NE.

Note 1 — For ERP created with stacked VLAN services, only NNIs can be added as ERP path endpoints.

Note 2 — Before creating ERP with stacked VLAN services, the port/LAG mode must be Network and Bind type must be ERP, associated with that particular VLAN. To achieve this:

- From the Equipment view, chose a port. Right- click on the port, and choose Properties. The Physical Port form opens.
- Choose the Network value for the Mode parameter.
- Choose the ERP value for the Bind Type parameter.
- Port → L2 Network Interfaces → VLAN, delete the VLAN association in which the ERP needs to be created
- Port → L2 Network Interfaces → VLAN, add it to the stacked VLAN with the Bind Type value as ERP.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Ring Element, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Ring Element from the contextual menu.

5 Choose an OmniSwitch site from the Select Network Elements window to create an Ethernet Ring Element.

6 Click on the OK button. The Ethernet Ring Element (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Ring Element (Ethernet Ring) on the drop-down menu in the Manage Service Tunnels window. Click on the Search button to display a list of the existing ring elements.

9 Select the ring element you want to configure and click on the Properties button.

The Ethernet Ring Element (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Description
- Administrative State
- Guard Time (centiseconds)
- Revert Time (minutes)
- Ring Protection Link Type
- Name
- Service ID
- AIS Meg Level

The ID and Site ID are only configurable when you are creating a new Ethernet Ring Element.

11 Click on the Path Endpoints tab button to configure the Path Endpoints.

12 Perform one of the following:

a If you are configuring an existing Ethernet Ring Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Ring Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Ring Path Endpoint, click on the Create button. The Ethernet Ring Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Path Endpoint Type

The Path ID parameter is only configurable when you are creating a new Ethernet Ring Path Endpoint.

14 If you are configuring an existing Ethernet Ring Path Endpoint, go to step 22.

15 Click on the Port tab.

16 Click on the Select button. The Select Member Port form opens.

17 Click on the Search button to list the available ports. Choose the port to use for the Ethernet ring path endpoint.

18 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form displays the selected member port.

Note 1 — You must select a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner or None. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The Ethernet Ring Path can be a LAG or port.

19 Configure the parameters:

- Path ID
- Path ID

20 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form closes.

The Path Endpoints tab displays the new Ethernet Ring Path Endpoint in the list.

21 Repeat steps 3 to 20 for the other Ethernet Ring Path Endpoint you need to create, if required.

22 Click OK. A dialog box appears.

23 Click Yes to close the Ethernet Ring Element form.

24 Click on the Protected Services tab button to view and specify the services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add a standard or stacked VLAN service:

i Click on the Add button. The Select Service window opens.

ii Click on the Search button to display a list of services available to include in this path. Only standard and stacked VLAN services can be included.

iii Select the required service and click on the OK button.

The Select Service window closes and the service you chose is displayed in the list on the Services tab.

Note 1 — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

Note 2 — If ERP is created with standard VLAN service, then standard VLAN services for Release 6.4.4/6.6.2 NEs and IPM Enterprise VLAN services for Release 6.6.2 NEs can be added as Protected services.

Note 3 — If ERP is created with stacked VLAN service, then stacked/IPM stacked VKLAN services for 6.4.4/6.6.2 NEs can be added as Protected Services.

25 To edit or view Protected Services, click on the Properties button of a selected standard VLAN service. The Ethernet Ring Element (Edit) form opens with the General tab displayed.

26 Click on the Protected Services tab button. Select a service. The Protected Services (Edit) form opens. Click on the Properties tab to edit or view the Protected service.

27 To view collected statistics, click on the Statistics tab button. To collect statistics, click on the Collect button. See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

28 Click on the OK button. The Ethernet Ring Element (Edit) form closes.

Procedure 33-9 To create an Ethernet radio ring element on a 9500 MPR

Radio ring elements are supported on the 9500 MPR Release 3.1 or later devices.

Create the ERP topology

1 Right-click on a 9500 MPR NE, and select Properties from the drop-down menu. A Network Element [Edit] form opens with the General tab selected.

2 Click on the Radio Ring Component tab button.

3 Click on the Create button. The Radio Ring Component new Object [Create] form opens.

4 Configure the ID and Topology Name parameters.

5 Click on the Select button beside the East Port Name parameter. The Select East Port - Radio Ring Component - new Object form opens.

6 Choose a port for the east port and click on the OK button.

7 Click on the Select button beside the West Port Name parameter. The Select West Port - Radio Ring Component - new Object form opens.

8 Choose a port for the west port and click on the OK button.

9 Click on the OK button to save the changes and close the Radio Ring Component new Object [Create] form.

10 Click on the OK button to save the changes and close the Network Element [Edit] form.

Create the radio ring representation

11 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

12 Click on the Create button and choose Radio Ring from the contextual menu. The Radio Ring, new Object [Create] form opens with the General tab displayed.

13 Configure the following parameters:

- Mgr ID
- Auto-Assign ID
- Name
- Description
- Hold Time Down
- Guard Time

14 Click on the OK button to save the change and close the Radio Ring, new Object [Create] form.

Create the radio ring element

15 Choose Radio Ring [Ethernet Ring] in the drop-down menu in the Manage Service Tunnels window and click on the Search button to display a list of the radio ring elements.

16 Choose the radio ring element you want to configure and click on the Properties button. The Radio Ring [Edit] form opens with the General tab displayed.

17 Click on the Components tab button. The Radio Ring and Ring Element icons display.

18 Right-click on the Ring Element icon and choose Create Ethernet Ring Element from the contextual menu. The Select Network Elements [Edit] form opens.

19 Double-click on a Radio Ring. The Ethernet Ring Element new Object [Create] form opens.

20 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Topology Name
- Description
- CCM Hold Time Down (deciseconds)
- Guard Time
- Ring Protection Link Type
- R-APS Vlan ID
- MEG Level

21 Click on the OK button to save the change and close the Ethernet Ring Element new Object [Create] form.

Add other ring elements

22 As required, add other ring elements to the radio ring by performing the following:

i Right-click on the Ring Element icon on the Radio Ring [Edit] form and choose Add Existing Element from the contextual menu. The Select Elements form opens.

ii Click on the Search button to display a list of the existing radio ring elements.

iii Choose a radio ring element on click on the OK button.

iv Repeat the substeps above to add other ring elements.

Add the radio ring to a VLAN path

23 Perform Procedure 69-12 to create a VLAN path. Choose Ring Based as the VLAN path type to add the radio ring to the VLAN.

Create the service on the ERPS topology

24 Perform one of the following to create a service for the 9500 MPR:

a Perform Procedure 69-8 to create a 9500 MPR (dot1q) VLAN service.

b Perform Procedure 70-3 to create a Epipe VLL service.

c Perform Procedure 70-10 to create a Cpipe VLL service.

Note 1 — For VLL services, the terminating sites have to be manually added to the service. For VLAN services, the sites get auto-populated.

Note 2 — When you create the VLL or VLAN service for the 9500 MPR, select the Ring Based path type.

Procedure 33-10 To create an Ethernet Ring

This procedure describes how to create an Ethernet Ring and its associated Control VPLS and data services.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Ring from the contextual menu. The Ethernet Ring (Create) window opens.

4 Configure the following parameters:

- Mgr ID
- Auto-Assign ID
- Element ID
- Name
- Description
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Guard Time (deciseconds)
- Compatible Version

5 Click on the Apply button. The Ethernet Ring (Edit) window opens with the General tab displayed.

6 Click on the Components tab button.

7 Right click on Ring Elements and choose one of the following items from the contextual menu.

a Create Ethernet Ring Element.

i Perform steps 5 to 22 in Procedure 33-7 to create an Ethernet Ring Element. When you are done, the element will be displayed on the Components tab in Ethernet Ring form.

Note 1 — You must create a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The parameter values specified in step 4 are initially populated in the Ethernet Ring Element form when creating a ring element from the Components tab. However, you can change these as required.

ii Repeat step i to create the other required ring elements.

Note — You can create all the ring elements required for the ring in one step. See step 5 in Procedure 33-7.

iii Go to step 8.

b Add Existing Element.

i The Select Element window opens.

ii Click on the Search button and select an element.

iii Click OK.

The element will be displayed on the Components tab in Ethernet Ring form.

Note 1 — You must select a ring element for each site that will be part of the Ethernet ring.

Note 2 — The Ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — When you add an existing Ethernet endpoint, the parameter values specified in step 4 are not populated into the properties of that endpoint.

iv Repeat steps i to iii to select the other required ring elements.

8 Right click on Paths and choose Create Ethernet Ring Path from the contextual menu to create a path. The Ethernet Path (Create) form opens with the General tab displayed.

Note — You must create a path for each element in the ring. Each element (site) in the ring will therefore have two endpoints (from two different paths) associated with it.

9 Configure the parameters:

- Auto-Assign ID
- ID
- Description

10 Click on the Endpoints tab button to configure the endpoints for the path.

Perform one of the following:

Note — One and only one endpoint within the entire Ethernet ring must have its Ring Protection Link Type parameter configured as Ring Protection Link End. All other endpoints in the Ethernet ring must have this parameter set to a value of Normal.

a Manually enter the following parameters for Endpoints A and B.

- Path ID
- Ring Protection Link Type
- Administrative State
- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)
- Member Port

Note — Path endpoints cannot be administratively enabled if:

- the R-APS Tag or Member Port parameters are not configured
- a MEP is not configured on the path endpoint

b Select an available path endpoint on endpoints A and B.

i Click on the Select button in the Path Endpoint section. The Select Path Endpoint window opens.

ii Click on the Search button and select an available endpoint.

iii Click OK. The endpoint parameters are automatically populated.

11 Click on the CFM Continuity Check tab button to configure a CFM Test for the path.

12 Click on the Select button. The Select CFM Test window opens. Perform one of the following:

a Click on the Search button to list the available CFM tests.

i Select the required CFM test.

ii Click OK.

The Select CFM Test window closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

b Click on the Create button to create the required CFM test. The Global Maintenance Entity Group (Create) form opens, with the General tab displayed.

Note — The Initial CCM Interval for the CFM test you select or create must be set to either 10 ms or 100 ms, otherwise the subsequent MEP creation will fail. The 7210 SAS-E, 7210 SAS-M and 7210 SAS-X do not support the 10 ms value.

Refer to Procedure 38-6 for information on creating the test.

13 Click on the Intermediate Services tab button to view and specify the intermediate services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Create button. The Select Service window opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service window closes and the service you chose is displayed in the list on the Intermediate Services tab.

Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.

Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Create button. The Create button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

14 Right click on Interconnects and choose Create Ethernet Ring Interconnect from the contextual menu to create an interconnect. The Ethernet Ring Interconnect (Create) form opens.

15 Configure the parameters:

- Auto-Assign ID
- ID
- Description

16 Configure the Element A end node for the interconnect.

i In the Element A panel, click on the Select button next to the ID field and select a site from the Select Element - Ethernet Ring Interconnect form.

ii Configure the parameters:

- Type
- Interconnected Ethernet Ring Element
- Propagate Topology Change

17 Configure the Element B end node for the interconnect.

i In the Element B panel, click on the Select button next to the ID field and select a site from the Select Element - Ethernet Ring Interconnect form.

ii Configure the parameters:

- Type
- Interconnected Ethernet Ring Element
- Propagate Topology Change

18 Click OK. A dialog box appears.

19 Click Yes to close the Ethernet Ring (Create) form.

20 Create a Control VPLS for the Ethernet ring.

i Perform Procedure 71-1 to create the VPLS, just as you would create a regular VPLS.

ii Perform Procedure 71-3 to create an L2 Access Interface for each path endpoint in the Ethernet ring. Each site in the Control VPLS must therefore have two control L2 Access Interfaces.

When creating the L2 access interfaces, ensure the following requirements:

- The Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 10.
- The Outer Encapsulation Value and Inner Encapsulation Value for the port in each L2 Access Interface must be set to the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively that you used for the particular path endpoint in step 10. This defines the interface as a Control SAP for the Ethernet ring.

21 Create the VPLS data services required for the Ethernet Ring.

i Perform Procedure 71-1 to create the VPLS, just as you would create a regular VPLS. The VPLS data service must be a regular VPLS, I-VPLS, or B-VPLS type.

ii Perform Procedure 71-3 to create an L2 Access Interface for each path endpoint in the Ethernet ring. Each site in the VPLS data service must therefore have at least two L2 Access Interfaces.

When creating the L2 access interfaces, the Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 10.

Procedure 33-11 To discover service tunnels

Use this procedure to list all service tunnels objects (SDPs, Ethernet rings, Ethernet tunnels, other services, and so forth) that are currently used by the service you are querying.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria and click on the Search button. A list of services is displayed.
3. Select a service in the list and click on the Properties button. The Service (Edit) form opens with the General tab displayed.
4. Click on the Service Tunnels tab.
5. Click the Discover Service Tunnels button to re-populate the list.

   Any previously discovered service tunnels on the service are removed and an on-demand re-discovery of these is triggered.

   A confirmation dialog appears when the discovery is complete.
6. Click OK.
7. Click on an item in the list and the Properties button to view the object information.
8. Close the Service (Edit) form.

Procedure 33-12 To discover flow-through services

Use this procedure to list all other services that are currently using the object you are querying as a service tunnel. These are collectively referred to as flow-through services. Refer to the "Service tunnel overview" section for a list of applicable service tunnel objects.

1. Open the configuration form of the object you want to examine.
2. Click on the Flow-through Services tab.
3. Click the Discover Flow-through Services button to re-populate the list.

   Any previously discovered flow-through services are removed and a manual re-discovery of these is triggered.

   A confirmation dialog appears when the discovery is complete.
4. Click OK.

5 Click on a service in the list and the Properties button to view the service information.

6 Close the object's configuration form.

Procedure 33-13 To view and manage service tunnels and tunnel elements

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria from the drop-down menu. The list contains all object types that can be used as service tunnels, along with related service tunnel management objects. The listing is hierarchical and includes:

- Ethernet Ring Element
- Ethernet Tunnel Endpoint
- Service Tunnel
    - Ethernet Tunnel
    - Ethernet Ring
    - P2MP LSP
    - Service (Service Management)
        - IES Service
        - MPR VLL
        - Mirror Service
        - Optical Transport Service
        - VLAN Service
        - VLL
        - VPLS
        - VPRN
    - Tunnel (Service Tunnel Management)
- Steering Parameter
- Tunnel Selection Profile

Note — For all service tunnel objects except Service, the search will display all objects of that type, regardless of whether or not they are being used as a service tunnel.

If you want to see only those objects that are currently being used as a service tunnel, enable the check box for the "Used By a Service" configurable filter item that exists in the list form.

3 Click on the Search button. A list containing the selected object type is displayed.

Note — If you searched on Service (or on a specific service type) used as a service tunnel, be aware that the generated list contents are subject to change, depending on current usage and on when the last on-demand (manual) discovery was conducted. There is no auto-discovery for this listing.

In other words, only those services will be listed that were known to be used as service tunnels when the last discovery was conducted. Since the discovery is only updated on user demand, the list of services generated here may not be up to date.

Procedure 33-11 details the on-demand discovery of service tunnels (including a service used by another service as a tunnel).

4 Select a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

5 View or configure the parameters on the General tab, as required.

6 View the States and State Cause indicators, if applicable, for troubleshooting information, such as a failed OAM diagnostic.

7 Click on the other tab buttons to view information or modify the parameters.

Note — The following tab buttons are not available for IP/MPLS service tunnels if the source is a 7250 SAS-ES:

- Tests
- Maintenance
- Accounting
- Statistics

8 Save the changes and close the Tunnel (Edit) form.

9 Close the Manage Service Tunnels form.

Procedure 33-14 To run an OAM validation test on a service tunnel

An OAM validator test suite must be created for the tested entity. See chapter 78 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

3 Select a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

4 Click on the More Actions button and choose Validate.

If an OAM validator test suite is not associated to the service tunnel, a dialog box appears. Perform the following steps:

i Click on the OK button to associate the service tunnel with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

ii Configure the filter criteria. A list of OAM validator test suites appears.

iii Select a OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result (Edit) form.

14 Close the Tunnel (Edit) form.

15 Close the Manage Service Tunnels form.

Procedure 33-15 To view the service tunnel topology

1 Choose Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map opens.

2 View the topology map as required. See chapter 5 for information about using topology maps.

3 Close the topology map.

34 — Lawful Intercept

34.1 Overview

Lawful Intercept, or LI, is a term that describes the interception and monitoring of network subscriber traffic by authorized agencies for law-enforcement purposes. A subscriber whose traffic is intercepted using LI is called a target. LI target traffic is replicated by a service mirror that uses subscriber information as the match criteria. LI has the following characteristics.

- LI is not detectable by a target subscriber.
- LI-related traffic is delivered separately from other network traffic.
- LI-related alarms only appear for authorized LI users.
- LI configuration information is stored in a separate and encrypted file.
- LI uses SSL security for data encryption, server authentication and message integrity between the 5620 SAM server and the single-user GUI clients or client delegate servers.

LI functions are managed separately from other 5620 SAM functions. LI mirroring is a special type of service mirroring that requires the following:

- on each LI NE in a mirror service:
    - SSH user security
    - an LI user profile
    - a user account that has LI privileges
- on the 5620 SAM:
    - SSL on the single-user GUI clients, client delegate servers and JMS server
    - a user account that has LI privileges
    - an assigned liMgmt scope of command role
    - an LI mediation policy

LI management requires a dedicated user authorization level. The 5620 SAM LI configuration forms, parameters, mirror services, and mirrored traffic appear only for a user with LI privileges, who can perform the following:

- create, configure, and view LI sources that use IP, MAC, SAP, and subscriber filters
- view LI-related alarms
- configure LI mediation policies
- modify the LI user password

Caution — An LI user password cannot be modified unless it is known. When an LI user password is not known, the LI user account is unavailable.

See chapter 72 for more information about mirror service management. See chapter 9 for more information about user privileges and scope of command roles.

Security

The 5620 SAM admin user, or an operator with an assigned admin scope of command role, must create an LI user account to be used for LI configuration. A user with the admin scope of command can perform only the following LI functions:

- Create an LI user scope of command profile and associate a non-admin user account with the LI profile.
- Configure an LI user profile that is restricts the LI user to LI activities only and does not allow system administrator activities.
- Create a password for the LI user.
- Configure CLI and SNMP access for the LI user account.

The 5620 SAM admin user cannot perform the following LI functions:

- Assign LI privileges to a user that is associated with the admin profile.
- View LI-related alarms.
- Delete an LI user.
- View, create, modify, or delete LI objects.
- View or modify LI mediation policies.

The following conditions apply to LI users and LI user groups:

- LI configuration requires the liMgmt scope of command role.
- The liMgmt role can be assigned to only one scope of command profile.
- A scope of command profile that has an assigned liMgmt role can include other roles except for the admin role.
- You cannot change the scope of command profile assignment for a user group when the profile includes the liMgmt role.
- An LI user group must be created as an LI user group; you cannot change a non-LI user group to an LI user group
- You cannot change an LI user group to a non-LI user group.
- A user account can have the liMgmt or the admin role, but not both.
- A user that belongs to an LI user group cannot be changed to a non-LI user.
- An LI span of control profile restricts LI user access to specific NEs.

34.2 Workflow to configure LI

The following is the sequence of high-level activities required to configure LI for the 5620 SAM.

1. Enable SSH security on each NE that is to perform an LI function. For more information about configuring SSH, see chapter 14.

2. Enable SSL security between the 5620 SAM main server and single-user GUI clients, and between the 5620 SAM main server and client delegate servers. For more information about configuring SSL security, see chapter 10.

3. Plan the 5620 SAM LI user-account creation according to the requirements for LI user access to other 5620 SAM functional areas.

4 As the 5620 SAM admin user, perform the following steps to create an LI user on the 5620 SAM. See Procedure 34-1 for more information.

   i Create a 5620 SAM LI scope of command profile that has an assigned liMgmt role.

   ii Create a 5620 SAM LI user group that is associated with the new scope of command profile.

   iii Create a 5620 SAM LI user account and assign it to the new user group.

5 If required, create an additional NE LI user account using the 5620 SAM GUI. See Procedure 34-7 for more information.

6 Provide the credentials for the 5620 SAM LI user account to the authorized LI administrator or LI user.

7 As the LI user, change the password of the 5620 SAM LI user account so that it is unknown to the 5620 SAM admin user. See Procedure 9-28 in chapter 9 for more information.

8 As the NE admin user, perform the following steps using a CLI to create an LI user on the NE.

   i Create an LI user profile on the NE. See Procedure 34-2 for information about creating an NE user profile using a CLI.

   ii Create an LI user account on the NE that is associated with the LI user profile. See Procedure 34-3 for information about creating an NE user account using a CLI.

9 Provide the credentials for the LI NE user account to the LI user.

10 As the LI user, perform the following steps.

   i Change the password of the LI NE user account so that it is unknown to the NE admin user. See Procedure 34-4 for more information.

   ii Create a 5620 SAM LI mediation policy for the NE that uses SSH for CLI sessions and secure file transfers. See Procedure 34-5 for more information.

   iii Specify whether the NE stores the LI source configuration locally or reconfigures the LI sources after a reboot. See chapter 10 for information about saving LI source configurations.

   iv Use the 5620 SAM to enable NE discovery for LI. See Procedure 34-6 for more information.

   v Configure LI mirror services. See chapter 72 for information about configuring mirror services.

   vi Configure the LI Filter Lock to configure who can modify base IPv4 and MAC filters referenced by an LI Source. See Procedure 34-8 for more information.

   vii As required, view LI user and system logs to monitor LI activity. See chapter 9 for more information about accessing user and system logs.

34.3 5620 SAM LI configuration procedures

This section describes how to configure LI on the 5620 SAM and on an NE.

Procedure 34-1 To create an LI user account on the 5620 SAM

Note — You require 5620 SAM admin user privileges to perform this procedure.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Profile (security) from the object drop-down list.

4 Click on the Create button. The Scope of Command Profile (Create) form opens with the General tab displayed.

5 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

6 Assign one or more scope of command roles to the profile. Perform the following steps.

i Click on the Roles tab button.

ii Click on the Add button. The Select Scope Of Command Role(s) - ScopeOfCommandProfile form opens.

iii Select one or more roles to include in the scope of command profile.

Note 1 — One of the roles you choose must be the liMgmt role.

Note 2 — You cannot include the admin role in an LI scope of command profile.

Note 3 — The 5620 SAM allows the creation of only one scope of command profile that contains the liMgmt role.

iv Click on the OK button. The Select Scope of Command Role(s) - ScopeOfCommandProfile form closes and a dialog box appears.

v Click on the OK button.

vi Click on the OK button. The Scope of Command Profile (Create) form closes.

7 Click on the User Groups tab button.

8 Click on the Create button. The User Group (Create) form opens with the General tab displayed.

9 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

10 Perform the following steps to assign the new LI scope of command profile to the user group.

i Click on the Select button beside the Profile ID field in the Scope of Command panel. The Select Scope of Command Profile - User Group form opens.

ii Select a profile from the list and click on the OK button. The Select Scope of Command Profile - User Group list form closes and the User Group (Create) form is refreshed with the scope of command profile information.

11 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button beside the Profile ID field in the Span of Control panel. The Select Span of Control Profile - User Group form opens.

ii Select a profile from the list and click on the OK button. The Select Span of Control Profile - User Group list form closes and the User Group (Create) form is refreshed with the span of control profile information.

12 Click on the OK button. The User Group (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

13 Click on the Users tab button. The User (Create) form opens.

14 Configure the parameters:

- User Name
- Description
- User State
- E-mail Address
- Password Change Required
- User Password
- Confirm Password
- Valid Client IP address
- Enable IP Address validation

15 Perform the following to associate the user with the newly created LI user group.

i Click on the Select button beside the User Group parameter. The groupName - User list form opens.

ii Choose the new LI user group from the list and click on the OK button. The groupName - User list form closes and the User (Create) form is refreshed with the user group information.

16 Click on the OK button. The User (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

17 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 34-2 To create an NE LI user profile using CLI

Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 15.

2 Enter the following commands in sequence at the prompt to create an NE user profile. The following is a sample configuration:

```
configure system security profile li-prof ↵
default-action deny-all ↵
li ↵
 entry 10 ↵
 match "configure li" ↵
 action permit ↵
 exit ↵
 entry 20 ↵
 match "exit" ↵
 action permit ↵
 exit ↵
 entry 30 ↵
 match "help" ↵
 action permit ↵
 exit ↵
 entry 40 ↵
 match "back" ↵
 action permit ↵
 exit ↵
 entry 50 ↵
```

```
match "show li" ↵
action permit ↵
exit ↵
entry 60 ↵
match "info" ↵
action permit ↵
exit ↵
entry 70 ↵
match "configure system security user" ↵
action permit ↵
exit ↵
entry 80 ↵
match "admin save" ↵
action permit ↵
exit ↵
exit ↵
admin save ↵
```

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 34-3 To create an LI user account on an NE using a CLI

Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 15.

2 Enter the following commands in sequence at the prompt to create an LI user:

```
configure system security snmp ↵
```

To specify the SNMP access group configuration, perform one of the following:

a For NE releases prior to 8.0 R7, type:

access group *LI_group* security-model usm security-level privacy context li exact read li-view write li-view notify iso ↵

b For NE releases 8.0 R7 to 8.0 R9 and 9.0 R1 to 9.0 R2, type:

access group *LI_group* security-model usm security-level privacy context li exact read iso write iso notify iso ↵

c For NE releases 8.0 R10+ and 9.0 R3+, type:

access group "*LI_group*" security-model usm security-level privacy read "iso" write "iso" notify "iso" ↵

access group "*LI_group*" security-model usm security-level privacy context "li" exact read "li-view" write "li-view" notify "iso" ↵

exit all ↵

configure system security user *LI_username* ↵

password *LI_password* ↵

access console li snmp ↵

snmp group *LI_group* ↵

console member *LI_profile* ↵

console no member default ↵

exit all ↵

admin save ↵

where
LI_group is the name of the LI user group on the NE
LI_usename is the name of the LI user account on the NE
LI_password is the password for the LI user account on the NE
LI_profile is the name of an LI user profile; see Procedure 34-2 for information about creating an LI user profile

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 34-4 To configure NE LI user security

Perform this procedure to change the password for an LI user account on an NE and to configure LI user authentication and SNMP data encryption on the NE.

Note — You require NE LI user privileges to perform this procedure.

1 Use the NE LI user account to open an SSH session on the NE. See chapter 15 for information about opening an SSH session on an NE.

2 Enter the following command to obtain the SNMP engine ID of the NE.

`show system info ↵`

The SNMP engine ID is displayed.

3 Record the SNMP engine ID for use in the following steps.

4 Log in to a 5620 SAM main server, client delegate server, or single-user client station using an appropriate user account.

Note 1 — If you are logging on to a main server or client delegate server station, you must log in as the samadmin user.

Note 2 — If you are logging on to a 5620 SAM single-user client station, you must log in as a local administrator, or as the user that installed the client.

5 Open a console window.

6 Navigate to the *install_dir*/nms/bin directory

where *install_dir* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on Solaris, or C:\5620sam\client on Windows

7 Perform the following steps to generate an MD5 authentication key for the NE LI user account. An authentication key is used to create an encrypted authentication password.

i Perform one of the following.

- On a Solaris station, enter the following at the CLI prompt:

`./nmsclient.bash password2key MD5` ***`password engine_ID`*** **↵**

- On a Windows station, enter the following at the CLI prompt:

`nmsclient.bat password2key MD5` ***`password engine_ID`*** **↵**

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the authentication key.

ii Record the key value for use later in the procedure.

8 Perform the following steps to generate an MD5 DES privacy key for the NE LI user account. A DES privacy key is used to encrypt the SNMP packets for additional security.

i Perform one of the following.

- On a Solaris station, enter the following at the CLI prompt:

./nmsclient.bash password2key MD5 *password engine_ID* ↵

- On a Windows station, enter the following at the CLI prompt:

nmsclient.bat password2key MD5 *password engine_ID* ↵

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the DES privacy key.

ii Record the key value for use later in the procedure.

9 Close the console window.

10 Enter the following commands in sequence at the CLI prompt to change the LI user password and to configure LI security for the user account:

configure system security user *username* ↵

password *new_LI_password* ↵

snmp ↵

authentication md5 *authentication_key* privacy des-key *DES_privacy_key* ↵

exit all ↵

admin save ↵

where
LI_group is the name of the LI user group on the NE
LI_usename is the name of the LI user account on the NE
new_LI_password is the new password for the LI user account on the NE
authentication_key is the MD5 authentication key value generated for the NE LI user in step 7
DES_privacy_key is the DES privacy key value generated for the NE LI user in step 8

11 Close the SSH session.

Procedure 34-5 To configure LI mediation

Perform this procedure to create an LI mediation policy that enables the creation of source objects for an LI service mirror.

Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the LI Mediation Security tab button.

3 Click on the Create button. The LI Mediation Policy (Create) form opens.

4 Click on the Select button beside the User Name parameter to view a list of configured users. The Select Site User For SNMP Access form opens.

5 Select the NE LI user created in Procedure 34-3 from the list and click on the OK button. The user name is displayed on the LI Mediation Policy (Create) form.

6 The SNMP passwords in the 5620 SAM mediation policy must match the encrypted passwords generated for the NE LI user in Procedure 34-4. Perform the following steps to set the mediation-policy passwords.

- **i** Click on the Properties button. The NE User Configuration form opens.
- **ii** Click on the SNMPv3 tab button.
- **iii** Enable the Authentication Protocol parameter.
- **iv** Specify the password used to generate the authentication key in Procedure 34-4 for the New Authentication Password and Confirm New Auth Password parameters.
- **v** Enable the Privacy Protocol parameter.
- **vi** Specify the password used to generate the DES encryption key in Procedure 34-4 for the New Privacy Password and Confirm New Privacy Password parameters.
- **vii** Click on the OK button. A dialog box appears.
- **viii** Click on the Yes button. The NE User Configuration form closes.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Mediation Policy (Create) form closes and the Mediation (Edit) form reappears.

9 Click on the OK button. The Mediation (Edit) form closes.

Procedure 34-6 To enable NE discovery for LI

Perform this procedure to enable LI discovery of an NE. Before you can enable LI discovery for an NE, the NE must be successfully discovered. See chapter 14 for information about configuring NE discovery.

Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

2 Click on the Managed State tab button. A list of discovered NEs is displayed.

3 Choose an NE on which Procedures 34-2 and 34-3 have been performed, and click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

4 Click on the LI Mediation Security tab button.

5 Click on the Select button in the Dual Read Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

6 Choose the LI mediation policy created in Procedure 34-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

7 Click on the Select button in the Dual Write Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

8 Choose the LI mediation policy created in Procedure 34-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

9 Click on the Select button in the Dual Trap Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

10 Choose the LI mediation policy created in Procedure 34-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

11 Click on the OK button. The Node Discovery Control (Edit) form closes and the Discovery Manager (Edit) form reappears.

12 Click on the Resync Status tab button.

13 Click on the Search button. A list of NEs is displayed.

14 Choose the NE and click on the Resync button. The Resync Options form opens.

15 Select Choose MIB Entries and click on the Next button. The Choose MIB Entries list form opens.

16 Select all TIMETRA-MIRROR-MIB entries in the list and click on the Finish button.

Note — Resynchronizing only the TIMETRA-MIRROR-MIB entries resynchronizes only LI source objects and keeps the resynchronization time to the minimum required.

17 Click on the Close button. The Resync Options form closes and the Discovery Manager (Edit) form reappears.

18 Click on the OK button. The Discovery Manager (Edit) form closes.

Procedure 34-7 To create an additional NE LI user account using the 5620 SAM GUI

Note 1 — You require 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 34-6.

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The NE User (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- User Name
- Description
- Access

You must specify the li, snmp, and console values for the Access parameter.

Additional configurable parameters are displayed.

4 Configure the additional parameters:

- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Specify an MD5 authentication key for the Password parameter. See Procedure 34-4 for information about generating a user authentication key.

5 Perform the following steps to assign a console profile, if required.

- **i** Click on the Console Profiles tab button. The list of profiles numbered one through eight appears. A user can have up to eight console profiles.
- **ii** Use the Select button beside one of the Profile 1 through Profile 8 parameters to choose a console profile. See chapter 21 for information about creating console profiles.

6 Click on the SNMPv3 tab button.

- **i** Enable the Authentication Protocol parameter.
- **ii** Specify an authentication key generated using Procedure 34-4 for the New Authentication Password and Confirm New Auth Password parameters.
- **iii** Enable the Privacy Protocol parameter.
- **iv** Specify a DES encryption key generated using Procedure 34-4 for the New Privacy Password and Confirm New Privacy Password parameters.
- **v** Click on the OK button. A dialog box appears.
- **vi** Click on the OK button. The NE User (Create) form closes and the NE User Configuration form reappears.

7 Close the NE User Configuration form.

Procedure 34-8 To configure the LI Filter Lock

This procedure allows a 5620 SAM LI user to configure a parameter that will permit base IPv4 and MAC filters referenced by an LI Source to be modified or deleted. The LI Filter Lock parameter specifies who can modify the LI filters. The available options are:

- Locked: no users can modify the LI filters
- Unlocked For LI Users: only users with LI privileges can modify the LI filters
- Unlocked For All: all users can modify the LI filters

Note — You require 5620 SAM LI user privileges to view the LI Configuration Status tab and to perform this procedure.

1 Right-click on a discovered device in the Equipment navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form is displayed.

2 Click on the LI Configuration Status tab button.

3 Configure the LI Filter Lock parameter.

4 Click OK to apply the configuration and close the Network Element (Edit) form.

Procedure 34-9 To configure LI NAT Source

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of mirror services appears.

3 Choose a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button. A list of mirror service sites are displayed.

5 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

6 Click on the LI NAT Sources tab button.

7 Click on the Configure LI Source Configuration button.

8 Click on the Ethernet Header tab button.

9 Configure the parameters:

- Source MAC Address
- Destination MAC Address
- EtherType

10 Click on the L2 Aware Subscribers tab button.

11 Click on the Create button. The LI Source NAT L2 Aware Subscriber (Create) form opens.

12 Configure the Subscriber ID and Intercept ID parameters.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The LI Source NAT L2 Aware Subscriber (Create) form becomes a tab.

15 Click on the OK button. The LI Source NAT L2 Aware Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

16 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

17 Click on the LI NAT Sources tab button. The Ethernet Header tab is displayed.

18 Click on the Dual Stack Lite LSN Subscribers tab button.

19 Click on the Create button. The LI Source Dual Stack Lite LSN Subscriber (Create) form opens.

20 Configure the parameters:

- Routing Instance ID
- IP Address
- Prefix Length
- Intercept ID

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The LI Source Dual Stack Lite LSN Subscriber (Create) form becomes a tab.

23 Click on the OK button. The LI Source Dual Stack Lite LSN Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

24 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

25 Click on the LI NAT Sources tab button. The Ethernet Header tab is displayed.

26 Click on the Classic LSN Subscribers tab button.

27 Click on the Create button. The LI Source Classic LSN Subscriber (Create) form opens.

28 Configure the parameters:

- Routing Instance ID
- IP Address
- Prefix Length
- Intercept ID

29 Click on the OK button. A dialog box appears.

30 Click on the OK button. The LI Source Classic LSN Subscriber (Create) form becomes a tab.

31 Click on the OK button. The LI Source Classic LSN Subscriber (Create) tab closes and the Mirror Service (Edit) form reappears with the Sites tab displayed.

32 Click on the Apply button. A dialog box appears.

33 Click on the Yes button.

34 Close the Mirror Service (Edit) form.

35 Close the Manage Mirror Services form.

Procedure 34-10 To enable or disable use of a secure channel for LI users

Perform this procedure to enable or disable use of an SSL connection for LI users and to make HTTPS requests over the XML OSS interface and the 5620 SAM GUI.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Search for the following XML tag. The secure channel check for LI Users can be enabled or disabled.

```
<liConf
```

```
liUserRequireSSL="value"
```

where *value* is set to true or false to enable or disable the secure channel check for LI users.

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the value defined is updated.

35 — IPsec

35.1 IPsec overview

The 5620 SAM supports the configuration of IPsec VPRN services, which are generically called IPsec VPNs. An IPsec VPN enables the secure extension of a corporate VPN over uncontrolled or untrusted private and public networks. The ISA-IPSEC MDA on the 7750 SR, Release 6.1 or later, provides IPsec tunneling and encryption between sites.

You can use the 5620 SAM to configure IPsec sessions and the security associations that are required in a bi-directional IPsec tunnel. You can configure multiple IPsec tunnels for a VPRN.

5620 SAM IPsec session configuration supports the following:

- encryption methods such as DES, 3DES, AES-128, AES-192, and AES-256
- authentication and hashing methods such as HMAC-MD5 and HMAC-SHA1
- key distribution methods such as IKE shared secret with PFS, and manual exchange
- key generation algorithms such as Diffie-Helman
- IPsec modes
- shared secret authentication
- NAT traversal
- DPD for the IPsec tunnel

An IPsec VPN service includes IPsec tunnels that terminate on IES or VPRN IPsec gateways. These gateways support L3 forwarding through an interface that connects to an IPsec tunnel. You can use the 5620 SAM to configure VPRN services to which individual hosts connect over the Internet to an IES or VPRN IPsec gateway. You can configure one or more tunnel interfaces in a VPRN service, and can configure multiple tunnel security profiles for each tunnel interface.

IKE policies are used to negotiate IPsec security associations, or SAs, between IPsec peers. AN SA is a relationship between two or more IPsec peers that defines how the peers communicate securely. IKE policies are exchanged between IPsec peers to negotiate a secure communication channel; they specify how traffic is encrypted between source and destination sites in an IPsec VPN by establishing a shared security policy using authentication keys.

IPsec transform policies specify the protocol for the IPsec authentication header and the encryption protocol for the encapsulating security payload, or ESP, and define the attributes that are used to secure the data.

After an IPsec peer initiates an IPsec session, there are two main phases:

- authentication and protection of IPsec peer identities and negotiation of matching IKE SA policies between peers to establish a secure channel for negotiating IPsec SAs in the next phase
- IPsec SA parameter negotiation and establishment of matching peer SAs

After the second phase, the IPsec peers exchange data over the IPsec tunnel according to the IPsec parameters in the IKE and IPsec transform policies.

You can create a tunnel template to configure shared IPsec transforms and IKE policies. Each IPsec peer configuration can include the following:

- one or more configured IPsec transforms
- one IKE policy
- one unique IPsec tunnel
- one tunnel filter defined in the IPsec tunnel configuration

Each IPsec tunnel between IKE peers is identified by a unique remote peer IP address or a unique local IP address.

You can use the IPsec Application Function Manager to create and manage end-to-end IPsec components to form a secure VPN. See section 35.2 for more information.

The 5620 SAM OSSI supports IPsec VPN configuration.

IPv6 IPsec

OSPFv3 authentication requires IPv6. IPv6 IPsec requires the following:

- IPsec transport mode —required because the NE acts as an OSPFv3 authentication host
- IPsec static security association—defines the SPI values, algorithms, protocol and keys to be used, and requires the same configuration at each end of the tunnel
- AH and ESP
- MD5 and SHA1

BFD

You can use BFD for static LAN-to-LAN IPsec tunnels on the 7750 SR-c4, 7750 SR-7, 7750 SR-12, and 7750 SR-c12. The following is the configuration information for implementing BFD over static LAN-to-LAN IPsec tunnels:

- You can have only one BFD session between a source/destination address pair.
- Each tunnel can be associated with only one BFD session. However, one or more tunnels, to a maximum of 500, can be associated with same BFD session.
- If one BFD session is associated with multiple tunnels, the tunnel that carries the BFD traffic must be operationally up before any of the other tunnels can be operationally up.
- When the 5620 SAM does not receive BFD packets from a peer before the detection time expires or a signal down notification is sent from a remote peer, the BFD session is considered down. When the 5620 SAM sets the associated IPsec tunnels in a down state, 5620 SAM performs the following:
  - sends a Delete Payload message to each remote peer from each associated tunnel and SA
  - removes the state and table entries from each associated tunnel and SA

35.2 IPsec VPN

You can create and manage the association between IPsec components, public and private services, to form a secure VPN. See “Typical applications for IPsec corporate services” in this section for the typical applications of an IPsec VPN.

You use the IPsec VPN step forms to perform the following:

- Configure the corporate service type.
- Enable the link between the corporate and secure service.
- Choose an NE service site.
- Configure the secure VPRN service.
- Configure the delivery service.
- Choose the Tunnel group.
- Create the policy.
- Deploy the IPsec VPN.

Tunnel types

Table 35-1 lists the tunnel types that you can create for an IPsec VPN.

Table 35-1 Tunnel types

Tunnel type	7750 SR, Release 6.0	7750 SR, Release 7.0 or later	7210 SAS
Dynamic (site-to-site)		✓	
Dynamic (soft client)		✓	
Static	✓	✓	✓

The 5620 SAM creates the following after the successful creation of an IPsec VPN, regardless of the tunnel type:

- a secure VPRN service and NE sites
- the IES or VPRN delivery service and NE sites
- if you specify that the secure and corporate services are to be linked, a composite service that contains the corporate and secure services

The 5620 SAM performs specific configuration actions after the successful creation of an IPsec VPN, depending on the tunnel type. See Procedures 35-15 to 35-17 for more information.

Typical applications for IPsec corporate services

Figure 35-1 shows one public L3 VPRN service that is associated with the corresponding private VPRN service. The private VPRN service belongs to a larger private VPRN. The public service can be a VPRN or IES service. The private service can only be a VPRN service.

Figure 35-1 Static IPsec tunnel

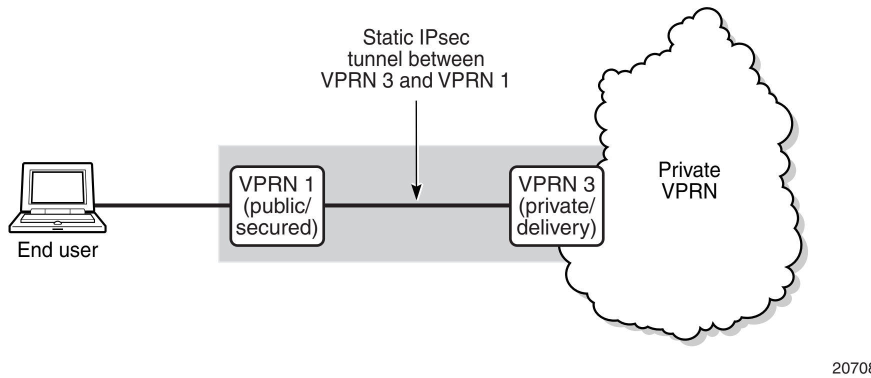


Figure 35-2 shows two public L3 VPRNs, VPRN 1 and VPRN 2, which are connected to the private, secure service VPRN 3 through an IPsec gateway. The public services can be VPRN or IES services. The private service can only be a VPRN service.

Figure 35-2 IPsec tunnels for a site

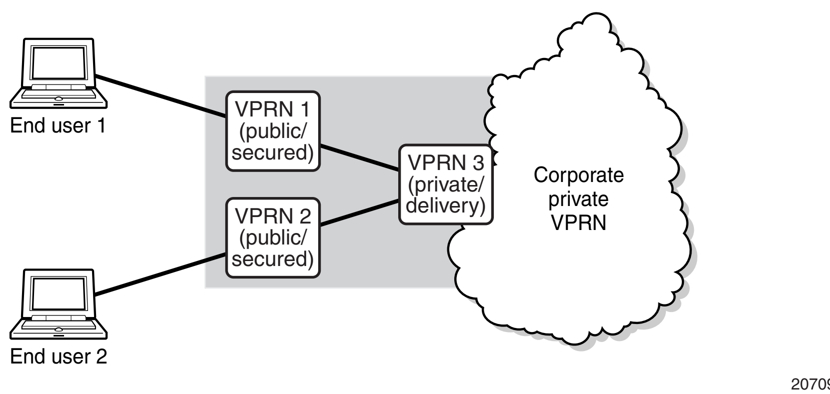


Figure 35-3 is the same as Figure 35-1, but Figure 35-3 shows IPsec tunnels across multiple sites. Site A, Site B, and Site C are part of the private service VPRN 4. For the site, there is a secure IPsec tunnel between a public service and a private service. The public services can be L3 VPRN or L3 IES services. The private service can only be a VPRN service.

Figure 35-3 IPsec tunnels for multiple sites

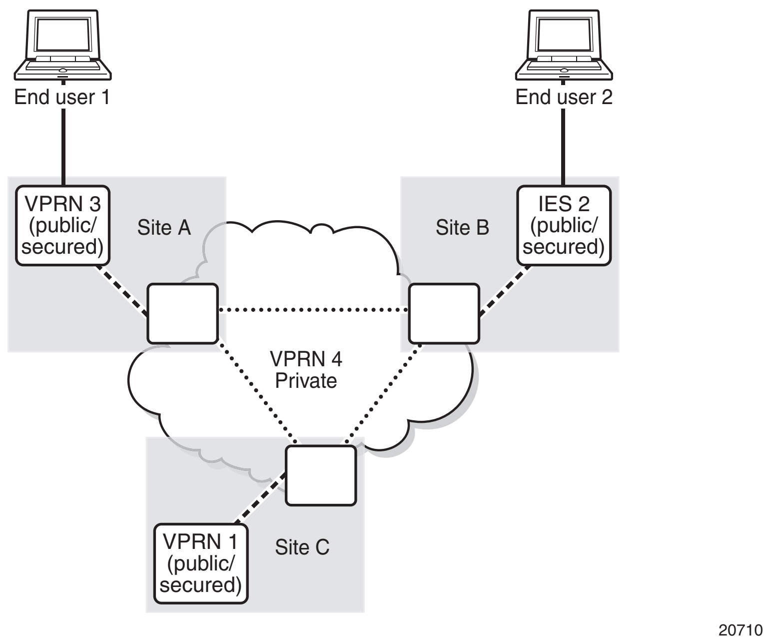
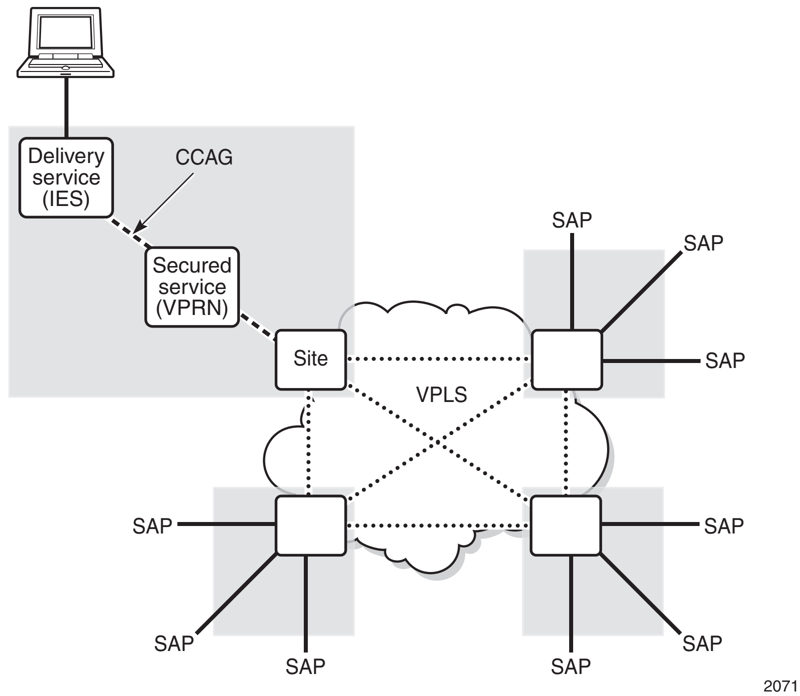


Figure 35-4 shows a private VPRN that is connected to a corporate network and a VPLS that is the corporate network. The public IES and private VPRN service are connected to VPLS network through a CCAG or SCP. CCAG connects the private VPRN to the VPLS network.

Figure 35-4 IPsec VPN in a corporate network

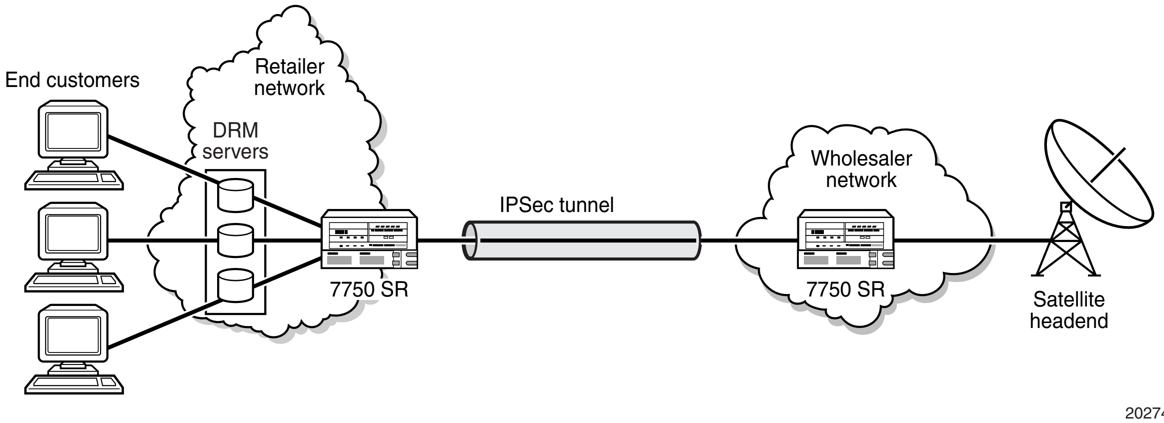


35.3 Sample video wholesale IPsec configuration

Larger providers or a cooperative of smaller providers often unite to provide a video headend to avoid the costs of investing in a satellite headend locations on their own ground station, to provide tripleplay features. Each retail subscriber can purchase content from this single station and receive it over IP. However, encryption is required so that the signal cannot be understood if intercepted.

Figure 35-5 shows a sample video wholesale configuration with a high-speed encrypted tunnel.

Figure 35-5 Sample video wholesale configuration



35.4 Workflow to configure and manage an IPsec configuration

See section 35.5 for the workflow to configure and manage an IPsec configuration using the IPsec VPN step forms.

1 Provision the ISA-IPSEC MDA on the 7750 SR, Release 6.1 or later. See chapters 16 and 17 for more information about IPsec equipment configuration.

- **i** Create or configure ISA-Tunnel groups.
- **ii** Assign the active and backup tunnel group members to the ISA-Tunnel groups.

2 Configure an IKE policy. See Procedure 35-1 for more information.

3 Configure an IPsec transform policy. See Procedure 35-2 for more information.

4 If your network will include shared IPsec transform and IKE policies, then configure an IPsec tunnel template. See Procedure 35-4 for more information.

5 Configure an IPsec security policy. See Procedure 35-5 for more information.

6 If you are configuring IPsec on a VPRN, then create the private-facing tunnel interface. See Procedure 35-6 for more information.

- **i** Create a private IPsec SAP.
- **ii** Configure ingress and egress policies, if required.

7 Create the public-facing tunnel interface. See Procedure 35-7 for more information.

- **i** Create an L3 access interface on an IES or VPRN. See chapters 73 and 74 for more information about creating an L3 access interface.
- **ii** Define the IPsec public SAP for the L3 access interface.
- **iii** Specify the IPsec gateway, if required, on the 7750 SR, Release 7.0 or later.

8 If you are configuring IPsec on a VPRN, then create IPsec tunnels on the VPRN tunnel interface. See Procedure 35-8 for more information.

9 Configure the static route.See Procedure 30-20 in chapter 30 for more information.

35.5 Workflow to configure and manage an IPsec configuration using the IPsec VPN

1 Create a corporate service and, if required, a service template. See Table 35-2 and the *5620 SAM Scripts and Templates Developer Guide* for more information.

2 Create an IPsec VPN. See Procedure 35-10 for more information.

3 Select the NE service sites for the IPsec VPN. See Procedure 35-11 for more information.

4 Create or select the secure VPRN service for the IPsec VPN. See Procedure 35-12 for more information.

5 Create or select the delivery service for the IPsec VPN. See Procedure 35-13 for more information.

6 Select the tunnel group for the IPsec VPN. See Procedure 35-14 for more information.

7 Assign policies and configurations to the IPsec VPN.

   i If you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2 of Procedure 35-14, then see Procedure 35-15 for more information.

   ii If you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2 of Procedure 35-14, then see Procedure 35-16 for more information.

   iii If you chose Static for the Tunnel Type parameter in step 2 of Procedure 35-14, then see Procedure 35-17 for more information.

8 Deploy the IPsec VPN.

35.6 Workflow to enable BFD over a static LAN-to-LAN IPsec tunnel

1 Create an tunnel interface on a VPRN, as described in Procedure 35-6.

2 Create an IPsec tunnel on the VPRN tunnel interface, as described in Procedure 35-8.

3 Enable BFD for the static LAN-to-LAN IPsec tunnel, as described in Procedure 35-9.

4 Assign a BFD service and interface that can be used for the BFD session on the IPsec tunnel.

35.7 General IPsec procedures

The following procedures describe how to perform general 5620 SAM IPsec configuration tasks, such as policy creation. See section 35.8 for IPsec VPN procedures.

Procedure 35-1 To configure an IKE policy

1. Choose Policies→ISA Policies→IKE from the 5620 SAM main menu. The IKE Policy form opens.

2. Perform one of the following:

   a. Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IKE Policy (Edit) form opens with the General tab displayed.

   b. Click on the Create button. The IKE Policy (Create) form opens with the General tab displayed.

3. Configure the parameters:

   - Auto-Assign ID
   - ID
   - Version
   - Description
   - Mode
   - Diffie-Hellman (DH) Group
   - Perfect Forward Secrecy (PFS)
   - PFS DH Group
   - Authentication Algorithm
   - Authorization Method
   - Encryption Algorithm
   - Internet Security Association and Key Management Life Time (seconds)
   - IPsec Life Time (seconds)

4. Click on the NAT Traversal tab button.

5. Configure the parameters:

   - NAT Traversal
   - Keep Alive Interval
   - Force Keep Alive

6. Click on the DPD tab button.

7. Configure the parameters:

   - Dead Peer Detection (DPD)
   - Interval
   - Max Retries

   The Interval and Max Retries parameters are not configurable if the Dead Peer Detection (DPD) parameter is set to Disabled.

8. Click on the Apply button.

9. Click on the General tab button.

10 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

11 Close the IKE Policy (Create) form.

12 Close the IKE Policy form.

Procedure 35-2 To configure an IPsec transform

1 Choose Policies→ISA Policies→IPSec Transform from the 5620 SAM main menu. The IPSec Transform form opens.

2 Perform one of the following:

  a Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IPSec Transform (Edit) form opens with the General tab displayed.

  b Click on the Create button. The IPSec Transform (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Authentication Algorithm
- Encryption Algorithm

4 Click on the Apply button.

5 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

6 Close the form.

7 Close the IPSec Transform form.

Procedure 35-3 To create an IPsec static security association

1 Choose Policies→ISA Policies→IPSec Static Security Association from the 5620 SAM main menu. The IPSec Static Security Association Policies form opens.

2 Click on the Create button. The IPsec Static Security Association (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Static SA Name
- Direction
- Protocol
- Authentication Algorithm
- Authentication Key Type
- Authentication Key
- Security Parameter Index
- Static SA Description

4 Click on the Apply button.

5 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

6 Close the form.

7 Close the IPsec Static Security Association (Create) form.

Procedure 35-4 To create an IPsec tunnel template

1 Choose Policies→ISA Policies→IPSec Tunnel Template from the 5620 SAM main menu. The IPSec Tunnel Template Policies form opens.

2 Click on the Create button. The IPSec Tunnel Template (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Reverse Route
- Replay Window

4 Click on the IPSec Transforms tab button.

5 Click on the Select button in the Transform ID 1 to Transform ID 4 panels. The Select Transform ID *1_4* IPSec Tunnel Template list form opens.

6 Choose an entry and click on the OK button. The Select Transform ID *1_4* IPSec Tunnel Template list form closes.

7 Click on the General tab button.

8 Click on the Apply button.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

10 Close the form.

11 Close the IPSec Tunnel Template form.

Procedure 35-5 To create an IPsec security policy

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.
3. Choose a VPRN service.
4. Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.
5. Click on the Sites tab.
6. Choose an entry and click on the Properties button. The VPRN Site (Edit) form opens with the General tab displayed.
7. Click on the IPSec Security Policies tab button.
8. Click on the Create button. The IPSec Security Policy (Create) form opens with the General tab displayed.
9. Configure the parameters:
   - Auto-Assign ID
   - Security Policy ID
10. Click on the IPSec Security Policy Entries tab button.
11. Click on the Create button. The Security Policy Entry (Create) form opens.
12. Configure the Name parameter.
13. Configure the Local Address Option parameter.
14. Perform one of the following.
    a. If you set the Local Address Option parameter to IP Address in step 13, configure the following parameters:
       - IP Address
       - Prefix Length

    b. If you set the Local Address Option parameter to None or Any, go to step 15.
15. Configure the Remote Address Option parameter.
16. Perform one of the following.
    a. If you set the Remote Address Option parameter to IP Address in step 15, configure the following parameters:
       - IP Address
       - Prefix Length

    b. If you set the Remote Address Option parameter to None or Any, go to step 17.

17 Click on the OK button. The Security Policy Entry (Create) form closes.

18 Repeat steps 8 to 17 to add additional IPSec security policy entries.

19 Click on the OK button. The IPSec Security Policy (Create) form closes. A dialog box appears.

20 Click on the OK button.

21 Close the VPRN Site (Edit) form.

22 Close the VPRN (Edit) form.

23 Close the Manage Services form.

Procedure 35-6 To create a tunnel interface on a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Tunnel Interfaces tab button.

6 Click on the Create button. The Tunnel Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured IP MTU (Octets)

8 Configure a port for the interface.

i Click on the Port tab button.

ii Click on the Select button to choose a port to associate with the tunnel interface. The Select Terminating Port - Tunnel Interface form opens.

iii Specify a filter for the search, if required, and click on the Search button.

iv Select a port from the list and click on the OK button. The Select Terminating Port - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the selected port information displayed.

v Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- SAP Description
- SAP Administrative State

Note 1 — You can configure the 5620 SAM to automatically assign lowest unused outer encapsulation value by enabling the Auto-Assign ID parameter.

Note 2 — You can set the Auto-Assign ID parameter to be the default parameter for dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

Note 3 — Private and public tunnel connection points support only dot1 Q encapsulation.

9 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

ii Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - Tunnel Interface form opens.

iv Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the ingress QoS policy information displayed.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - Tunnel Interface form opens.

vi Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the egress QoS policy information displayed.

10 Click on the Schedulers tab button to configure scheduling. Otherwise, go to step 12.

Note — The Schedulers tab is configurable only if you assign a port to the SAP in step 8.

11 Perform the following:

i Configure the Aggregate Rate Limit (kbps) parameter.

Note 1 — The Aggregate Rate Limit (kbps) parameter is configurable only when you enable the Assign Aggregate Rate Limit check box, and there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

ii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - Tunnel Interface form opens.

iii Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - Tunnel Interface form closes, and the Tunnel Interface (Create) form refreshes with the ingress scheduler information displayed.

iv Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - Tunnel Interface form opens.

v Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - Tunnel Interface form closes, and the Tunnel Interface (Create) form refreshes with the egress scheduler information displayed.

vi Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy - Tunnel Interface form opens.

vii Choose an ingress policer control policy and click on the OK button. The Select Policer Control Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form refreshes with the ingress policer information displayed.

viii Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy - Tunnel Interface form opens.

ix Choose an egress policer control policy and click on the OK button. The Select Policer Control Policy - Tunnel Interface form closes and the Tunnel Interface (Create) form refreshes with the egress policer information displayed.

x Go to step 12.

12 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - Tunnel Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the ingress IPv4 ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - Tunnel Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Tunnel Interface form closes and the Tunnel Interface (Create) form reappears with the egress IPv4 ACL filter information displayed.

13 Assign an IP address to the tunnel interface.

i Click on the Addresses tab button.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The Tunnel Interface (Create) form reappears with the assigned IP addresses displayed.

14 Configure a GRE tunnel on the Tunnel Interface, if required.

i Click on the GRE Tunnels tab button.

ii Click on the Create button. The GRE Tunnel (Create) form opens.

iii Configure the parameters:

- Name
- Description
- DSCP
- Destination Address
- Remote Address
- Local Endpoint Address
- Backup Remote Address

iv Click on the Select button on the Delivery Service panel to choose a delivery service for the GRE tunnel. The Select Delivery Service - GRE Tunnel form opens.

v Select a delivery service and click on the OK button. The Select Delivery Service - GRE Tunnel formcloses and the GRE Tunnel (Create) form reappears with the delivery service information displayed.

vi Click on the States tab button and configure the Administrative State parameter.

vii Click on the OK button. The GRE Tunnel (Create) form closes, and a dialog box appears.

viii Click on the OK button. The Tunnel Interface (Create) form reappears with the assigned GRE tunnel displayed.

15 Specify queue overrides by clicking on the Override Policy Items tab button. See chapter 47 for information about how to set queue overrides.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Tunnel Interface (Create) form closes, and the VPRN Service (Create) form reappears.

18 Repeat steps 6 to 16 to create another tunnel interface for the VPRN service.

Procedure 35-7 To create an IPsec gateway on an IES or VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select an IES or VPRN.

4 Click on the Properties button. The properties form for the service opens with the general properties of the service displayed on the General tab.

5 Click on the L3 Access Interfaces tab button.

6 Click on the Search button. A list of L3 access interfaces appears.

7 Choose the L3 access interface on which you want to create the IPsec gateway and click on the Properties button. The *Service* L3 Access Interface (Edit) form opens with the General tab displayed.

Note — The port configured on the L3 access interface must be a Tunnel Group SAP. This is the public-facing interface for an IPsec tunnel.

8 Click on the IPSec Gateway tab button.

9 Click on the Create button. The IPSec Gateway (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Name
- Pre Shared Key

11 Click on the Select button in the IKE Policy panel to associate an IKE policy with the IPSec gateway. The Select IKE Policy - IPSec Gateway list form opens.

12 Specify a filter for the search, if required, and click on the Search button. A list of IKE policies appear.

13 Choose a policy and click on the OK button. The Select IKE Policy - IPSec Gateway list form closes.

14 Click on the Select button in the IPSec Tunnel Template panel to associate an IPsec tunnel template with the IPsec gateway. The Select IPSec Tunnel Template - IPSec Gateway list form opens.

15 Specify a filter for the search, if required, and click on the Search button. A list of IPsec tunnel templates appear.

16 Choose an IPsec tunnel template and click on the OK button. The Select IPSec Tunnel Template - IPSec Gateway list form closes.

17 Select the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the Secure Service Id panel. The Select Secure Service Id - IPSec Gateway list form opens.

ii Specify a filter for the search, if required, and click on the Search button. A list of VPRN services appears.

iii Choose an entry and click on the OK button. The Select Secure Service Id - IPSec Gateway list form closes.

18 Select the tunnel interface on the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the Tunnel Interface Name panel. The Select Tunnel Interface Name - IPSec Gateway list form opens.

ii Click on the Search button. A list of tunnel interfaces appears.

iii Choose an entry and click on the OK button. The Select Tunnel Interface Name - IPSec Gateway list form closes.

19 Configure the Local Gateway Address parameter.

20 Click on the States tab button.

21 Configure the Administrative State parameter.

22 Click on the OK button. The IPSec Gateway (Create) form closes. A dialog box appears.

23 Click on the OK button to close the dialog box. The *Service* L3 Access Interface (Create) form reappears.

24 Click on the OK button to save the configuration and close the form.

25 A dialog box appears. Click on the OK button to close the dialog box.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button. The properties form for the service closes.

Procedure 35-8 To create an IPsec tunnel on a VPRN tunnel interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Tunnel Interfaces tab button.

6 Choose a tunnel interface and click on the Properties button. The Tunnel Interface (Edit) form opens.

7 Click on the IPsec Tunnels tab button.

Note — You must first assign a port to the tunnel interface for the IPsec Tunnels tab to appear.

8 Click on the Create button. The IPSec Tunnel (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- Replay Window
- Keying
- Local Gateway Address
- Remote Gateway Address

10 Click on the Select button beside the Security Policy ID parameter. The Select Security Policy - IPSec Tunnel list form opens.

11 Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

12 Choose an entry and click on the OK button. The Select Security Policy - IPSec Tunnel form closes.

13 Click on the Select button beside the Name parameter. The Select Service Name - IPSec Tunnel list form opens.

14 Specify a filter for the search, if required, and click on the Search button. A list of services appears.

15 Choose an entry and click on the OK button. The Select Service Name - IPSec Tunnel form closes.

16 Perform one of the following.

a If you set the Keying parameter to None in step 9, go to step 19.

b If you set the Keying parameter to Dynamic in step 9, go to step 17.

c If you set the Keying parameter to Manual in step 9, go to step 18.

17 Configure dynamic keying.

i Click on the Dynamic Keying tab button.

ii Click on the Select button beside the following parameters:

- Transform ID 1
- Transform ID 2
- Transform ID 3
- Transform ID 4

The Select Transform ID - IPSec Tunnel form opens.

iii Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

iv Choose an entry and click on the OK button. The Select Transform ID - IPSec Tunnel form closes.

v Click on the Select button beside the IKE Policy parameter. The Select IKE Policy - IPSec Tunnel list form opens.

vi Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

vii Choose an entry and click on the OK button. The Select IKE Policy - IPSec Tunnel form closes.

viii Configure the parameters:

- Pre Shared Key
- Auto Establish

ix Go to step 19.

18 Configure manual keying.

i Click on the Manual Keying tab button.

ii Click on the Create button. The IPSec Security Association (Create) form opens.

iii Click on the Select button in the Security Policy Entry panel. The Select Security Policy Entry - IPSec Security Association list form opens.

iv Click on the Search button. A list of policy entries appears.

v Choose an entry and click on the OK button. The Select Security Policy Entry - IPSec Security Association list form closes.

vi Configure the parameters:

- Direction
- Encryption Key
- Authentication Key
- SPI

vii Click on the Select button in the Transform panel. The Select Transform - IPSec Security Association list form opens.

viii Click on the Search button. A list of transform policies appears.

ix Choose an entry and click on the OK button. The Select Transform - IPSec Security Association list form closes.

x Click on the OK button. The IPSec Security Association (Create) form closes.

19 Click on the States tab button.

20 Configure the Administrative State parameter.

21 Click on the BFD tab button.

22 Configure the parameters:

- Designated
- Enabled

If you set the Enabled parameter to Enabled, go to step 23. Otherwise, go to step 28.

23 Click on the Select button beside the Service Name parameter. The Select BFD Service - IPsec Tunnel BFD form opens.

24 Configure the filter, if required, and choose a BFD service. The BFD service information appears for the Service Name, Service ID, and Site ID parameters.

25 Click on the Select button beside the Name parameter. The Select Interface - IPsec Tunnel BFD form opens.

26 Configure the filter, if required, and choose an interface. The interface name appears for the Name parameter.

27 Configure the Destination Address parameter.

28 Click on the OK button. The IPSec Tunnel (Create) form closes. A dialog box appears.

29 Click on the OK button.

30 Repeat steps 8 to 29 to add additional IPsec tunnels.

Procedure 35-9 To enable BFD for a static LAN-to-LAN IPsec tunnel

Note — BFD can only be enabled for the 7750 SR.

1. On the private side, use the CLI to specify a tunnel as the BFD tunnel and enable BFD on the tunnel. For example:

   ```
   config>service>vprn>ipsec-if>sap>tun>
   ```

   ```
   [no]bfd-enable [service-id] interface interface-name dst-ip
   ip-addr
   ```

   ```
   [no]bfd-designated
   ```

   See the 7750 SR documentation for more information about the CLI commands.

2. On the public side, use the CLI to configure the transmit interval. For example:

   ```
   config>service>vprn>if>
   ```

   ```
   bfd transmit-interval [receive receive-interval] [multiplier
   multiplier] [echo-receive echointerval]
   ```

   See the 7750 SR documentation for more information about the CLI commands.

3. Create a VPRN service. See chapter 74 for more information.

4. Create two VPRN L3 access interfaces. See chapter 74 for more information.

5. Create a tunnel interface on a VPRN, as described in Procedure 35-6.

6. Create an IPsec tunnel on a VPRN tunnel interface, as described in Procedure 35-8.

35.8 IPsec VPN procedures

The following procedures describe how to perform 5620 SAM IPsec configuration tasks using the IPsec VPN step forms.

Procedure 35-10 To create an IPsec VPN

Note — The 5620 SAM does not support the creation of IPsec VPNs when language localization is active. See "Localized language support" for more information about language localization.

1 Configure a corporate service. Table 35-2 lists where to find information about each corporate service type.

Table 35-2 Corporate service types

Corporate service	See chapter
Apipe	70
Cpipe	
Fpipe	
Ipipe	
VPLS	71
IES	73
VPRN	74
VLAN	69

2 If required, configure one or more service templates. Table 35-2 lists where to find more information.

3 Choose Create→IPsec VPN from the 5620 SAM main menu. The Create IPsec VPN step form opens.

4 Configure the parameters:

- Auto-Assign ID
- IPsec VPN Name
- Description
- Service Type
- Link Corporate and Secured Service

5 To select a corporate service, perform the following, otherwise, go to step 6.

  i Click on the Select button beside the Corporate Service ID parameter. The Select Corporate Service - IPsec VPN form opens. Only the specific service type, as set by the Service Type parameter, is listed.

  ii Filter the corporate services, if required, and select a corporate service.

  iii Click on the OK button to close the Select Corporate Service - IPSec VPN form. The Corporate Service ID and Corporate Service Name parameters display the service ID and service name for the selected corporate service on the Create IPsec VPN step form.

6 Click on the Next button on the Create IPsec VPN step form. The Select Service Sites step form opens. Perform Procedure 35-11 to select the service sites.

Procedure 35-11 To select a service NE site for an IPsec VPN

This procedure selects the NE site for the IPsec VPN.

1 Perform Procedure 35-10 to create an IPsec VPN.

2 Perform one of the following:

  a To choose an existing service site, configure the filter and click on the Search button. A list of service sites appears. Go to step 7.

  b To create a service site, go to step 3.

3 Click on the Create button. The Manage Equipment form opens.

4 Configure the filter, if required, and click on the Search button. A list of NEs appears.

5 Select a NE and click on the OK button. The NE appears in the Select Service Sites step form.

6 Repeat steps 3 to 5 to add another NE site.

7 Select an NE site and click on the Next button. The Create/Select Secure VPRN Service step form opens. Perform Procedure 35-12 to:

- select a service
- create a service
- create a service from a template

Procedure 35-12 To create or select a secure VPRN service for an IPsec VPN

1 Perform Procedures 35-10 and 35-11.

2 Perform one of the following:

a To select a service, go to step 3.

b To create a service, go to step 7.

c To create a service from a template, go to step 12.

Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

3 Click on the Select Service button. The Select Service form opens.

4 Configure the filter, if required, and click on the Search button. A list of services appear.

5 Select a service and click on the OK button. The service appears in the Create/Select Secure VPRN Service step form.

6 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

Go to step 15.

7 Click on the Create Service button.

8 Click on the Select button beside the Customer parameter. The Select Customer form opens.

9 Filter the customers, if required, and select a customer from the list.

10 Click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

Go to step 6.

12 Click on the Create Service From Template button. The Create Service From Template appears.

13 Filter the services, if required, and click on the Search button.

14 Select a service from the list and click on the OK button. Go to step 6.

15 Click on the Next button. The Create/Select Delivery Service(s) step form opens. Perform Procedure 35-13.

Procedure 35-13 To create or select a delivery service for an IPsec VPN

1 Perform Procedures 35-10 to 35-12.

2 Perform one of the following:

- a To select a delivery service, go to step 3.
- b To create a delivery service, go to step 8.
- c To create a service from a template, go to step 13.

Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

- d To remove a service, go to step 17.

3 Click on the Select Service button. The Select Service form opens.

4 Choose IES Service (IES) or VPRN Service (VPRN) from the drop-down menu, choose a filter, if required, and click on the Search button.

5 Select a service from the list and click on the OK button. The service appears in the Create/Select Delivery Service(s) list.

6 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

7 Repeat steps 3 to 6 to select another service. Go to:

- a step 8 to create a service
- b step 13 to create a service from a template
- c step 17 to remove a service
- d step 18 to select a tunnel group

8 Click on the Create Service button and choose VPRN or IES. The service appears in the Create/Select Delivery Service(s) list.

9 Click on the Select button beside the Customer parameter. The Select Customer form opens.

10 Choose a customer and click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

12 Repeat steps 8 to 11 to create another service. Go to:

a step 13 to create a service from a template

b step 17 to remove a service

c step 18 to select a tunnel group

13 Click on the Create Service From Template button and choose VPRN or IES. The Create Service Form Template appears.

14 Configure the filter, if required, and click on the Search button. A list of services appears.

15 Select a service template and click on the OK button.

16 Repeat steps 13 to 15 to create another service. Go to:

a step 17 to remove a service

b step 18 to select a tunnel group

17 If you perform this step, the service is removed without confirmation and there is no undo. Select a service in the Create/Select Delivery Service(s) list and click on the Remove Service button.

18 Click on the Next button. The Tunnel Group Selection step form opens. Perform Procedure 35-14.

Note — The Next button is not enabled until you perform steps 9 and 10 for each delivery service in the Create/Select Delivery Service(s) step form.

Procedure 35-14 To select a tunnel group for an IPsec VPN

1 Perform Procedures 35-10 to 35-13.

2 Select a service and configure the parameters by clicking in the panel and entering values or choosing an option:

Note 1 — The parameters are not part of the XML. In OSSI, you can create the ServiceSiteStructs and in the ServiceSiteStructs, you can create the IPsec VPN objects.

Note 2 — If the tunnel type is static, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

If the tunnel type is dynamic site-site, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address

If the tunnel type is dynamic soft client, the parameters that require configuration are:

- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address

- ISA-Tunnel Group
- Tunnel Type
- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

3 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

4 Repeat steps 2 and 3 for each service.

5 Click on the Next button. The Create Policy step form opens.

Perform Procedure 35-15 if you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2.

Perform Procedure 35-16 if you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2.

Perform Procedure 35-17 if you chose Static for the Tunnel Type parameter in step 2.

Note — The Next button is not enabled until you perform step 2 for each tunnel group in the Tunnel Group Selection step form.

Procedure 35-15 To assign policies and configurations for a dynamic site-to-site IPsec VPN

This procedure assumes you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2 of Procedure 35-14.

1 Perform Procedures 35-10 to 35-14.

2 Click on the Select button beside the IPsec Tunnel Template Policy ID parameter in the IPsec Tunnel Template panel. The Select IPsec Tunnel Template - IPsec VPN form opens.

3 Perform one of the following:

- **a** To select an IPsec tunnel template from the list, go to step 4.
- **b** To create an IPsec tunnel template, go to step 5.

4 Configure the filter, if required, click on the Search button. Go to step 10.

5 Click on the Create button. The IPsec Tunnel Template form opens. Perform steps 3 to 11 in Procedure 35-4.

6 Click on the Select button beside the Policy ID parameter in the IKE Policy panel. The Select IKE Policy - IPsec VPN form opens.

7 Perform one of the following:

- **a** To select an IKE Policy from the list, go to step 9.
- **b** To create an IKE Policy, go to step 8.

8 Click on the Create button and perform steps 3 to 12 in Procedure 35-1.

9 Select a Policy and click on the OK button.

10 Configure the Pre Shared Key parameter.

11 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 35-1)
  - an access interface is created
  - a tunnel interface is created
  - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 35-2)
  - an access interface is created
  - the IP address of the SAP is configured
  - a tunnel group with an auto-generated outer encapsulation as a public SAP is assigned
  - an IPsec gateway is created
  - the secure service is assigned
  - the tunnel interface of the secure service is assigned
  - the tunnel template is assigned
  - the IKE policy is assigned
  - the local gateway address is configured
  - the Pre Shared key is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 35-1: Secure VPRN service example

```
vprn 254 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-1" create
                sap ipsec-2.private:9 create
                exit
            exit
            service-name "VPRN service-310 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 35-2: VPRN delivery service example

```
vprn 255 customer 2 create
            interface "sam-auto-access-intf-1" create
                address 33.33.3.3/24
                sap ipsec-2.public:11 create
                    ipsec-gw "sam-auto-gateway-1"
                        default-secure-service 254 ipsec-interface
"sam-auto-ipsec-intf-1"
                        default-tunnel-template 1
                        ike-policy 1
                        local-gateway-address 33.33.3.2
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
    service-name "VPRN service-311 CPM_132_A (38.120.169.132)"
    no shutdown
exit
```

Procedure 35-16 To assign policies and configurations for a dynamic soft client IPsec VPN

This procedure assumes that you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2 of Procedure 35-14.

1 Perform Procedures 35-10 to 35-14.

2 Perform steps 2 to 9 in Procedure 35-15.

3 Click on the Select button beside the Displayed Name parameter. The Select Subscriber Authentication Policy - IPsec VPN form opens.

4 Perform one of the following:

- **a** To select a subscriber authentication policy from the list, go to step 6.
- **b** To create a subscriber authentication policy, go to step 5.

5 Click on the Create button. The Subscriber Authentication Policy (Create) form opens. See chapter 21 for information about creating a Subscriber Authentication Policy.

6 Select a subscriber authentication policy from the list and click on the OK button.

7 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 35-3)
    - an access interface is created
    - a tunnel interface is created
    - the IP Address of the SAP is configured
    - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 35-4)
    - an access interface is created
    - the IP address of the SAP is configured
    - the RADIUS authentication policy is assigned
    - a tunnel group with an auto-generated outer encapsulation as a public SAP is assigned
    - an IPsec gateway is created
    - the tunnel template is assigned
    - the IKE policy is assigned
    - the local gateway address is configured
    - the Pre Shared key is configured
    - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 35-3: Secure VPRN service example

```
vprn 260 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-4" create
                address 9.9.9.9/24
                sap ipsec-1.private:47 create
                exit
            exit
            service-name "VPRN service-316 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 35-4: VPRN delivery service example

```
vprn 261 customer 2 create
            interface "sam-auto-access-intf-4" create
                address 40.1.1.2/24
                authentication-policy "test"
                sap ipsec-1.public:42 create
                    ipsec-gw "sam-auto-gateway-4"
                        default-tunnel-template 1
                        ike-policy 2
                        local-gateway-address 40.1.1.1
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
    service-name "VPRN service-317 CPM_132_A (38.120.169.132)"
    no shutdown
exit
```

Procedure 35-17 To assign policies and configurations for a static IPsec VPN

This procedure assumes that you chose Static for the Tunnel Type parameter in step 2 of Procedure 35-14.

1 Perform Procedures 35-10 to 35-14.

2 Perform steps 3 to 6 in Procedure 35-15.

3 Configure the parameters:

- Pre Shared Key
- Replay Window
- Keying

If you set the Keying parameter to Manual, go to step 4. If you set the Keying parameter to Dynamic, go to step 6.

4 Configure the Manual Keying - Inbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Inbound

5 Configure the Manual Keying - Outbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Outbound

6 Perform one of the following:

a To select an IPsec transform policy from the list, go to step 8.

b To create an IPsec transform policy, go to step 7.

7 Click on the Create button and perform steps 3 to 12 in Procedure 35-1.

8 Select an IPsec transform policy and click on the OK button.

9 Configure the Auto Establish parameter.

Note — The Auto-Establish parameter is only configurable if dynamic keying is selected.

10 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and NE sites are created (see Code 35-5)
    - the IPsec security policy is created
    - a tunnel interface is created
    - a tunnel group with an auto-generated outer encapsulation as a private SAP is assigned
    - the IPsec tunnel is created
    - the security policy is assigned to the tunnel
    - the local and remote gateway addresses are configured
    - the delivery service is configured
    - the replay window is configured
    - the keying is configured
    - if set, auto establish is enabled
    - the static route is configured
    - the service name is configured
- the IES or VPRN delivery service and NE sites are created (see Code 35-6)
    - an access interface is created
    - a tunnel group with an auto -generated outer encapsulation as a public SAP is assigned
    - the IP address of the SAP is configured
    - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 35-5: Secure VPRN service example - Keying parameter set to Dynamic

```
vprn 252 customer 2 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip any
                        remote-ip any
                    exit
                exit
            exit
            ipsec-interface "sam-auto-ipsec-intf-32" create
```

```
                sap ipsec-1.private:46 create
                    tunnel "sam-auto-tunnel-32" create
                        security-policy 1
                        local-gateway-address 40.1.1.2 peer 2.2.2.2 delivery-service
253
                        replay-window 64
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "Test"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
            exit
            static-route 3.3.3.3/32 ipsec-tunnel "sam-auto-tunnel-32"
            service-name "VPRN service-308 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 35-6: VPRN delivery service example

```
vprn 253 customer 2 create
            interface "sam-auto-access-intf-32" create
                address 40.1.1.1/24
                sap ipsec-1.public:41 create
                    collect-stats
                exit
            exit
            service-name "VPRN service-309 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

36 — ISA-Video

36.1 ISA-Video overview

The 5620 SAM allows the equipment and services configuration of the following enhancements to multicast video service provided by the ISA-Video MDA module:

- Reliable Delivery/Retransmisson (RT) Proxy
- Fast Channel Change (FCC)
- Ad Insertion (ADI)

These features are supported on the 7750 SR and 7450 ESS, Release 7.0 R4 or later.

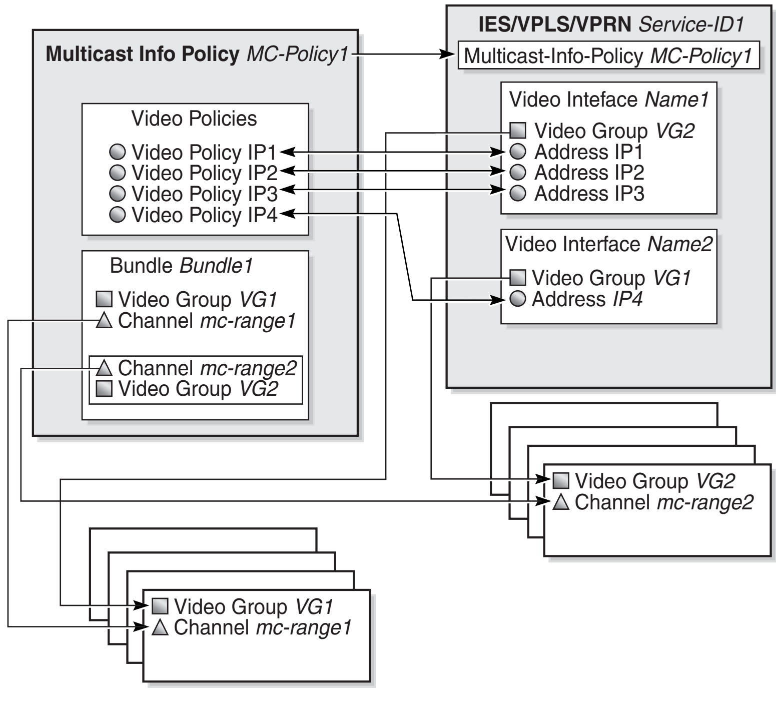
You can use the 5620 SAM to configure the required ISA-Video Groups and Members, as well as the associated multicast info policies. VPRN, IES, and VPLS services can then be configured for the customer video delivery.

These enhancements are provisioned in 5620 SAM in following three areas:

- A Video Group configuration to manage the ISA resources and service grouping.
- Multicast Information policy configuration parameters and objects to handle the RT, FCC and Ad insertion capabilities, including:
    - A Video Policy configuration under the Multicast Information Policy
    - Video parameters added to Multicast Bundles, Channels and Channel override configurations
- Video Interface configurations are added under VPRN/IES/VPLS services sites.

Figure 36-1 shows the relationship of these various elements and how they are associated through configuration.

Figure 36-1 ISA-Video configuration elements



A Video Interface within a service site can have up to eight IP addresses. The IP addresses assigned to a Video Interface determine which MultiCast Info Policy is applied. The Video Group you assign to the Video Interface determines which bundle/channel configuration inside the Multicast Info policy is applied to the interface. You also configure the ingress and egress QOS policies for the Video Interface using the Video Group.

If a request is received on a Video Interface for a channel not serviced by the Video Group associated with that specific Video Interface, then the request is considered invalid and is dropped. For example, in Figure 36-1, a request for mc-range2 received on IP1, IP2, or IP3 is invalid. A request for mc-range2 is only valid on IP4.

A Video Group manages the ISA-Video MDA resource and the configurations of the enhanced video functionality. You can assign a Video Group (for example, VG1 in Figure 36-1) for each Bundle, and this is the default Video Group for all of the channels in that Bundle. You can then apply specific configuration overrides for each channel within a Video Group assignment.

Up to four Video Groups (ID 1-4) can be configured on a single node. Each Video Group in turn, can have multiple primary video ISAs assigned to provide load balancing and redundancy protection. However, any specific video ISA can only be bound to one Video Group. The binding of a video ISA to the Video Group is referred as a Video Group Member.

Additional considerations for the Ad Insertion functionality:

- Ingress Ad Insertion channels are configured on the Video Interface configuration form.
- If Ad Insertion functionality is enabled on a Video Group, then the group can only have one Video Group Member.
- You can configure Zone Channels for egress Ad Insertion on each Ad Insertion channel configuration.
- Ad Insertion channels are not applicable to VPLS.

36.2 Workflow to configure and manage an ISA-Video configuration

1. Provision the ISA-Video MDA. See chapters 16 and 17 for more information about ISA-Video MDA equipment configuration.

2. Create or configure ISA-Video Groups and add members under the Video Groups. See Procedure 18-11 for more information.

3. Configure and distribute a global Multicast Information policy. Configure the channel bundle, channel range, channel overrides, and video interface for the node. See Procedure 49-4 for more information.

4. Create and enable a video interface for the VPLS, IES, or VPRN service. See procedures 36-1, 36-2, and 36-3 for more information.

36.3 ISA-Video procedures

The following procedures describe how to perform 5620 SAM ISA-Video configuration tasks.

Procedure 36-1 To add a Video interface to a VPRN site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPRN service.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3. Choose the required VPRN service and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4. On the navigation tree, click on the site to which you want to add the video interface; expand the entries for that site.

5. Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you choose a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button beside the corresponding fields. You can perform a search or choose the entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button and choose the required NE DoS Protection Policy from the list. You can also perform a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Go to step 12 if you are configuring ad insertion. Otherwise go to step 25.

12 Click on the ADI Channels tab and click on the Create button. The Video ADI Channel (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

14 Click on the Zone Channels tab and click on the Create button. The Video ADI ZoneChannel (Create) form opens.

15 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

16 Click on the OK button. The Video ADI ZoneChannel (Create) form closes, and a dialog box appears.

17 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

18 Repeat steps 14 to 17 to configure additional Zone Channels, if required.

19 Click on the OK button. The Video ADI Channel (Create) form closes, and a dialog box appears.

20 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

21 Click on the ADI (SCTE 30) Server tab and click on the Create button. The ADI (SCTE 30) Server (Create) form opens.

22 Configure the Server Address parameter.

23 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

24 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

25 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

26 Click on the OK button. The newly-configured Video Interface is displayed for the site.

27 Close the Manage Services form.

Procedure 36-2 To add a Video interface to an IES site

The 7710 SR and 7750 SR support the configuration of a video interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required IES service and click on the Properties button. The IES (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the video interface and expand the entries for that site.

5 Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Go to step 12 if you are configuring ad insertion. Otherwise go to step 25.

12 Click on the ADI Channels tab and click on the Create button. The Video ADI Channel (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

14 Click on the Zone Channels tab and click on the Create button. The Video ADI ZoneChannel (Create) form opens.

15 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

16 Click on the OK button. The Video ADI ZoneChannel (Create) form closes and a dialog box appears.

17 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

18 Repeat steps 14 to 17 to configure additional Zone Channels, if required.

19 Click on the OK button. The Video ADI Channel (Create) form closes and a dialog box appears.

20 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

21 Click on the ADI (SCTE 30) Server tab and click on the Create button. The ADI (SCTE 30) Server (Create) form opens.

22 Configure the Server Address parameter.

23 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

24 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

25 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

26 Click on the OK button. The newly-configured Video Interface is displayed for the site.

27 Close the Manage Services form.

Procedure 36-3 To add a Video interface to a VPLS site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the video interface and expand the entries for that site.

5 Right-click on the Video Interfaces and select Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Administrative State
- Group Number
- Associated Multicast Service ID
- RT Client Address
- Gateway Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter
- Ingress Mac Filter
- Egress Mac Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

9 Click on the Addresses tab and click on the Create button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Click on the OK button. The Video Interface (Create) form closes, and a dialog box appears.

12 Click on the OK button. The newly-configured Video Interface is displayed for the site.

13 Close the Manage Services form.

37 — Alarm management

37.1 Alarm management overview

The 5620 SAM converts SNMP traps from NEs and 5620 SAM events to alarms that are associated with the managed equipment, configured services and policies.

The alarm-based fault management system provides the following:

- the conversion of SNMP traps from NEs to alarms using the X.733 standard
- the correlation of alarms with equipment- and service-affecting faults
- updates to the managed-object operational status in near-real-time
- alarm policy control that allows a network administrator to specify how to process alarms and how to create and store the alarm logs
- point-and-click alarm management using the 5620 SAM GUI dynamic alarm list and object properties forms
- the ability to log the actions taken to correct the associated fault by adding notes to the alarm
- an alarm history for performing trend analysis

Figure 37-1 shows how the 5620 SAM manages alarms.

Figure 37-1 Alarm management

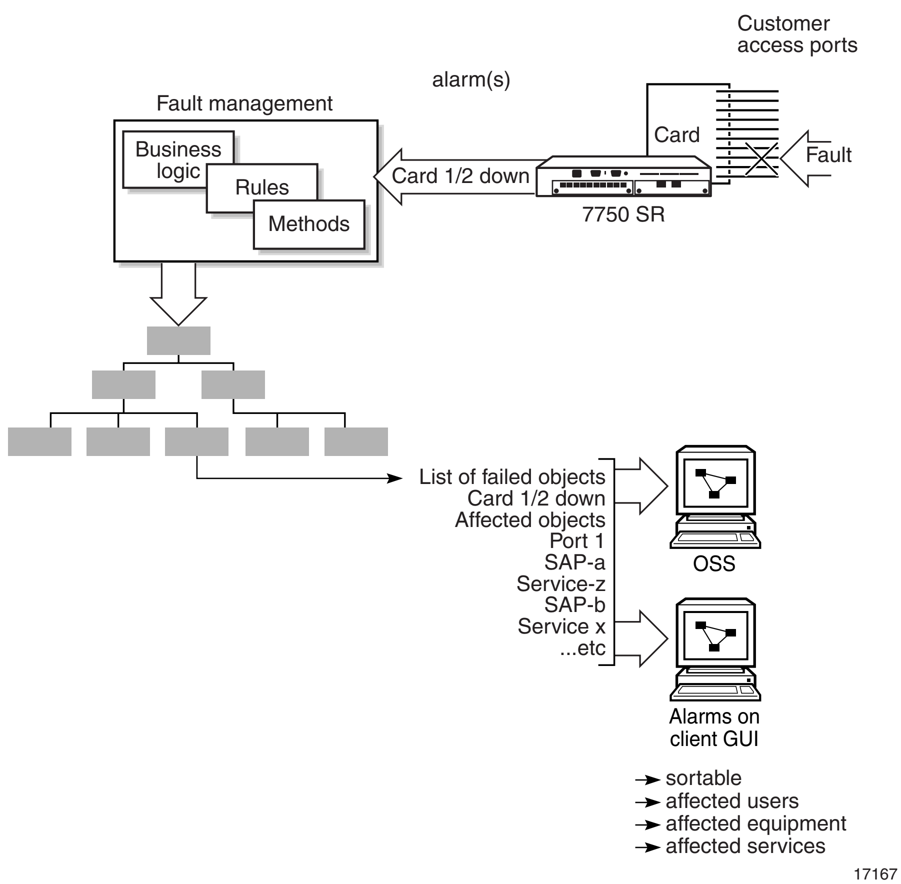
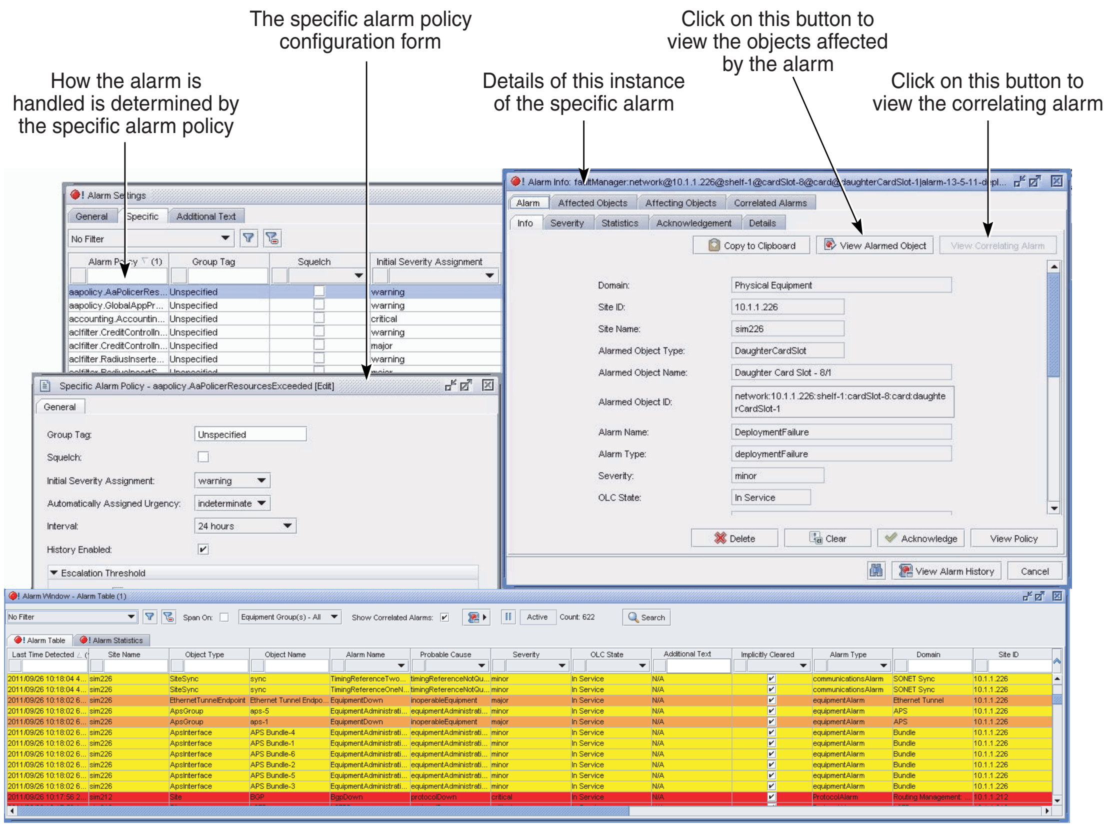


Figure 37-2 shows the following related alarm objects in the 5620 SAM GUI:

- an incoming alarm in the dynamic alarm list
- the alarm policy
- the alarm information form

Figure 37-2 Alarm relationships on the GUI



19620

You can view the history of one or more alarms using a 5620 SAM menu option, from the Alarm Info form, and using the View Alarm(s) History contextual menu option in the Alarm Window. From the Alarm Window, you can use the Historical Alarms button to open the Historical Alarms form, and can view the alarm history of an object by choosing the View Object(s) Alarm History contextual menu option.

Note — The View Alarm(s) History and View Object(s) Alarm History menu options are unavailable when more than 20 alarms are selected.

The following information is displayed on an Alarm Info form.

- Alarm tab—contains alarm information that includes the object, severity, statistics, and acknowledgement status.
- Affected Objects tab—contains a list of objects that are affected by the alarm. All alarms list the affected objects, even when correlation alarm suppression is enabled. See Figure 37-3 for how affected objects are determined.
- Affecting Objects tab—contains a list of objects that directly affect the object in alarm. See Figure 37-3 for how affecting objects are determined.
- Correlated Alarms tab—contains a list of correlated alarms. Correlated alarms are raised against other objects that are dependent on the alarmed object.

Alarm status, severity, and aggregation

Alarm status for the network is indicated in the navigation tree, the dynamic alarm list, and on the topology maps. You can use the navigation tree to view the status of an alarm raised against a specific object and to view the aggregated alarm status. The aggregated alarm status is also available on the Faults tab of an object property form.

Alarms are considered related or affecting when there is a relationship between objects. The 5620 SAM business logic determines that, for example, if a port goes down and the port is used by a SAP, a customer is affected by the port down alarm.

Figure 37-3 shows how aggregation, affecting, and affected alarms are determined.

Figure 37-3 Aggregation, affecting, and affected alarm inheritance

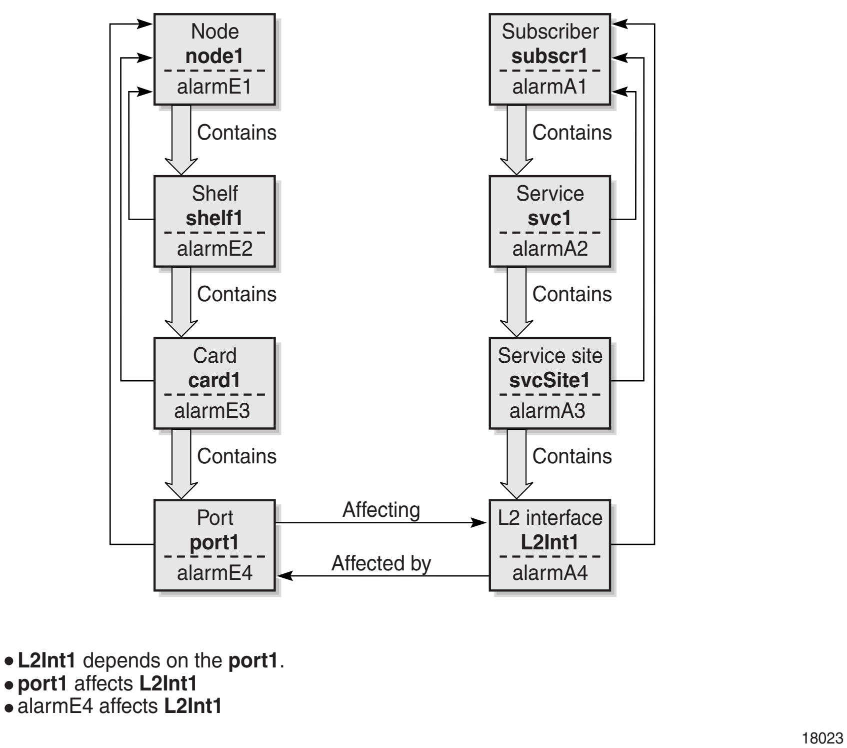


Table 37-1 shows the alarm relationships based on the example in Figure 37-3.

Table 37-1 Alarm relationships

Object	Object alarms	Affecting alarms	Aggregated alarms	Related object alarms
NE1	alarmE1	—	alarmE2 alarmE3 alarmE4	—
shelf1	alarmE2	—	alarmE3 alarmE4	—
card1	alarmE3	—	alarmE4	—
port1	alarmE4	—	—	alarmA4
subscr1	alarmA1	—	alarmA2 alarmA3 alarmA4	—
svc1	alarmA2	—	alarmA3 alarmA4	—
svcSite1	alarmA3	—	alarmA4	—
L2Int1	alarmA4	alarmE4	—	—

The 5620 SAM GUI uses color to indicate alarm severity. The color code is used consistently throughout the GUI, for example, in the navigation tree, dynamic alarm list, and topology maps. Table 37-2 lists the default alarm colors.

Table 37-2 Default 5620 SAM alarm colors

Alarm severity	Default color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Cyan
Condition	Mocha
Cleared/Normal	Green
Indeterminate	White
Information	Light blue

The following tabs are on the Faults tab of an object properties form.

- Object Alarms—contains information about the alarm as viewed from the dynamic alarm list. For example, shelf1 is the object, and alarmE2 is the object alarm.
- Affecting Alarms—contains information about the alarms on objects that are directly affecting this object. For example, alarmE4 on object port1 is affecting object L2Int1, because of the relationship between the L2 interface and port1.

- Aggregated Alarms—contains alarm information for objects below the listed object in the containment hierarchy. For example, object shelf1 contains two propagated alarms, alarmE3 and alarmE4, because the shelf contains card1 and port1.
- Alarms on Related Objects—contains information about the alarms that have an indirect relationship with the object. For example, alarmA4 is displayed in the Alarms on Related Objects tab for port1, because it is related to the fault condition on port1.

Figure 37-4 shows the alarm status information for an object in the navigation tree, the object properties form, and the associated alarm information form. You can use the alarm information form to view the affected objects, the affecting objects, and the correlated alarms.

Note — In the navigation tree, an aggregated alarm may be present when no child object in the tree has an alarm. This is because the navigation tree is a filter for different views. When you change the view using the drop-down menu; for example, from Equipment to Network, the aggregated alarm on the child object may appear.

Figure 37-4 Alarm status information in the navigation tree

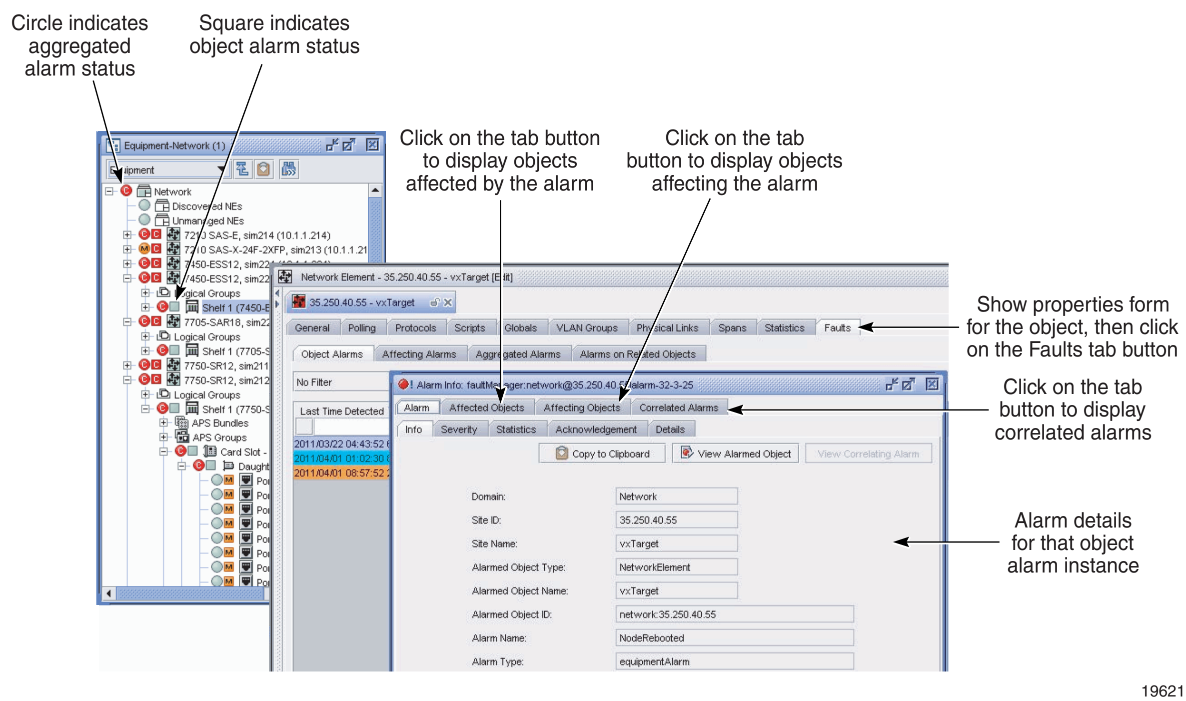


Figure 37-5 shows alarm and status information on a topology-map icon. See the *5620 SAM Troubleshooting Guide* for information about using topology maps for alarm management.

Figure 37-5 Alarm and status information on topology map icons

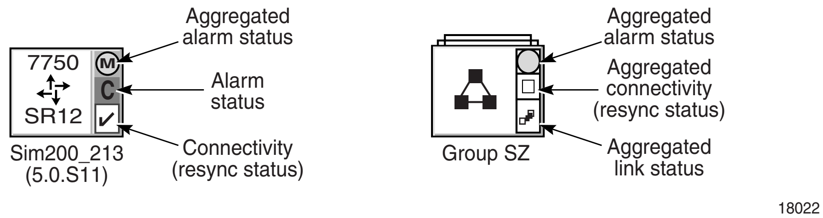
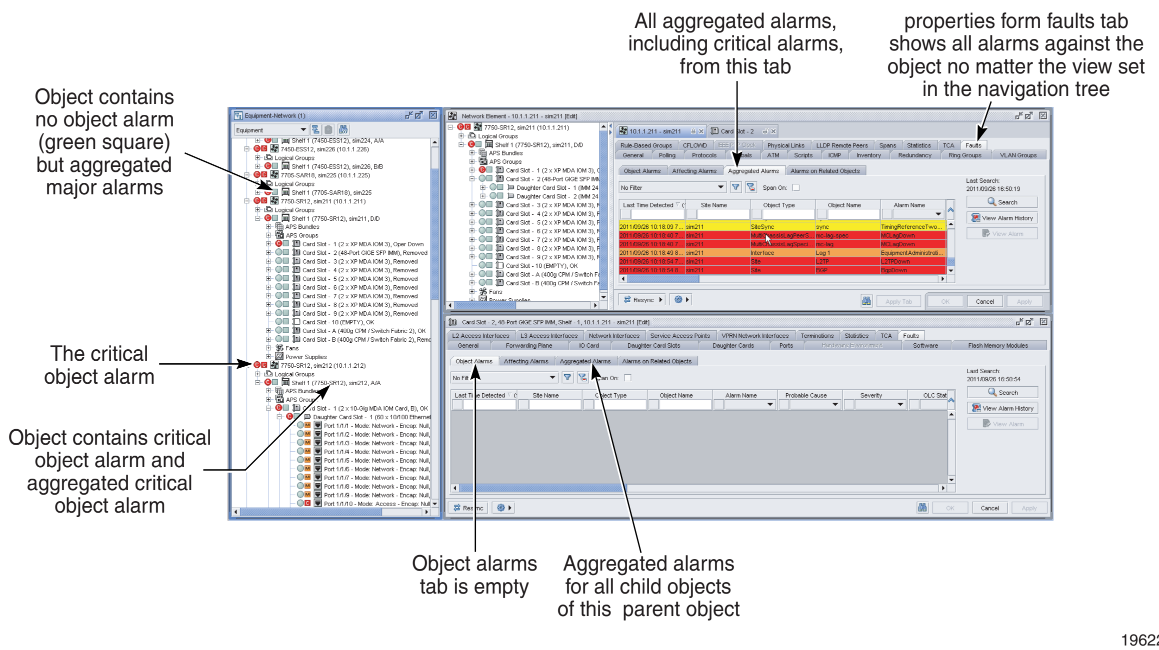


Figure 37-6 shows how to navigate from the aggregated or object alarms in the navigation tree to the Faults tab of an object properties form.

Figure 37-6 Navigating from the navigation tree to Faults tab on a properties form

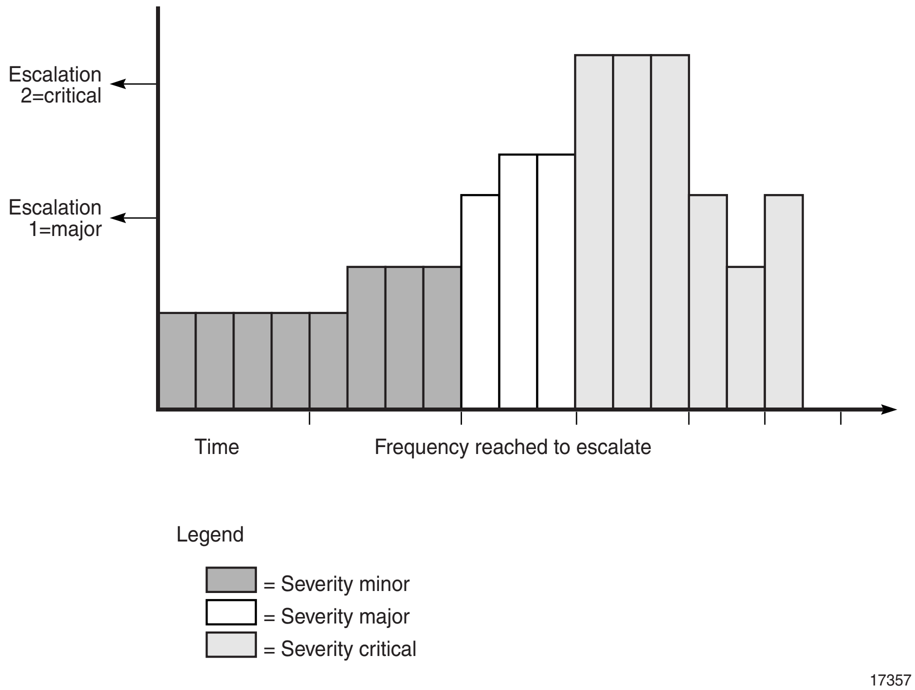


Alarm thresholds

The 5620 SAM provides tools to escalate and de-escalate the severity of alarms using alarm threshold measures that are configurable using specific alarm parameters, as described in Procedure 37-2.

Figure 37-7 shows an example of what happens when an alarm threshold escalation is reached, and a policy is applied. Figure 37-8 shows two escalation and two de-escalation policies applied to an alarm.

Figure 37-7 Alarm thresholds without de-escalation policies

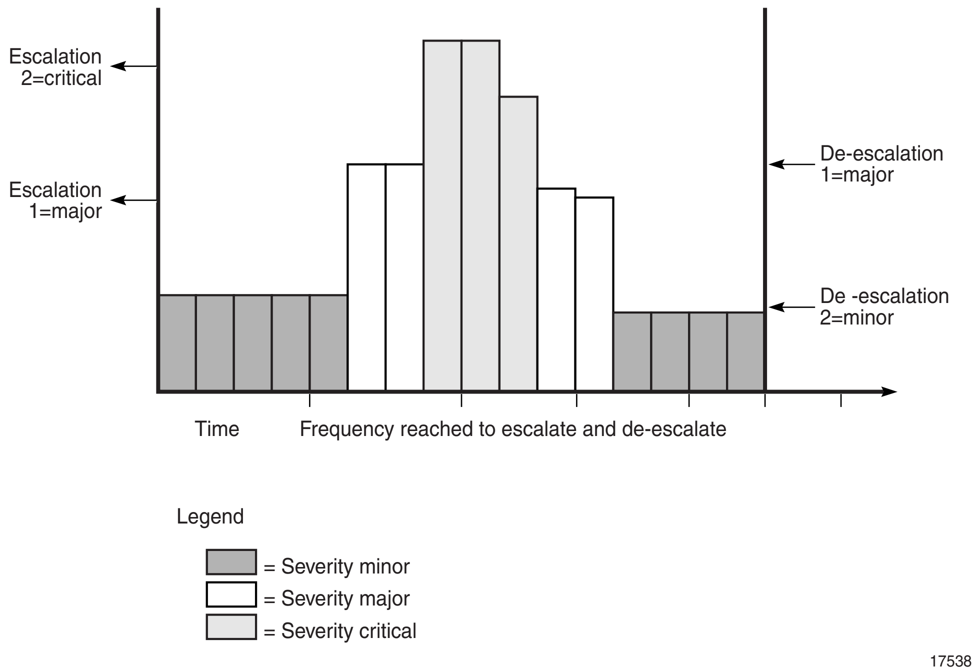


The preceding figure shows two escalation policies applied to an alarm. Escalation rules are applied when the number of instances of the alarm, also called the frequency, reaches the configured value. De-escalation rules are applied when the number of instances of the alarm drops below the configured frequency value. When the escalation value is reached, the alarm is escalated to the configured value. As shown in the figure, the first escalation is to major priority and then to critical priority. When the appropriate frequency to escalate and de-escalate is reached, the alarm is first escalated in severity and then de-escalated. However, if the alarm is deleted, then the frequency calculation is affected.

Note — When no de-escalation policy is applied, escalated alarms are not de-escalated once the frequency of the alarm drops below the alarm escalation threshold.

Figure 37-8 shows two escalation and two de-escalation policies applied to an alarm.

Figure 37-8 Alarm thresholds with de-escalation policies



Escalation policies are affected by the auto parameter of the global alarm deletion policy. See Procedure 37-1 for more information. When an escalation policy uses the “default when cleared” option, the escalation policy does not work. You must configure the parameter to a value other than “when cleared” to ensure the escalation policy is successful.

Alarm suppression

The 5620 SAM is designed to not raise alarms when numerous SNMP traps are sent in quick succession for the same type of event. This prevents alarm storms during intermittent outages in the network caused by bouncing NEs; for example, when links go up and down rapidly. The 5620 SAM continues to resynchronize the network, and if the bouncing NEs continue to send down state SNMP traps, the 5620 SAM eventually receives the trap and generates the appropriate alarm.

To indicate how often an alarm is raised, the number of occurrences of each instance of the alarm is tracked within the alarm record of the initial alarm. Click on the Statistics tab of an individual Alarm Info form to see how often the alarm was raised.

To cause alarm severity to escalate if an alarm reoccurs a specific number of times, use the threshold crossing alert functionality, as described in Procedure 37-2 using the Escalation parameter or the De-escalation parameter.

The 5620 SAM uses a process called trap throttling to prevent the 5620 SAM system from being overloaded with traps when a failure occurs. Trap throttling does not affect the sequencing of traps. The trap throttling process allows the 5620 SAM software to process traps when it has the time. As a result, the 5620 SAM software knows which traps the software missed and resynchronizes only those traps. Trap throttling is supported and configured through the CLI on each Alcatel-Lucent NE. See the Alcatel-Lucent NE System Management Guides for configuration instructions.

Correlated alarms

The 5620 SAM raises a correlated alarm when a fault condition on one object causes an alarm condition on another object. For example, when a port goes down, an alarm is raised against the port, which is the affected object, and each service that uses the port generates an alarm. The alarm information for the affected object includes the correlated alarms.

The 5620 SAM automatically adjusts the severity of correlating alarms to match the severity of correlated alarms. For example, in a case where a major correlating port alarm has one or more critical correlated service alarms, the 5620 SAM adjusts the severity of the correlated port alarm to critical. The correlating alarm cannot have a severity that is lower than the severity of the correlated alarms, however, the severity that is defined by a specific alarm policy takes precedence over the correlated severity. The 5620 SAM does not decrease the severity of correlating alarms when correlated alarms are cleared.

Note — Alarm correlation does not affect the severity of HIP alarms, or alarms that originate from an external EMS.

When the event that triggers an affected-object alarm is corrected and the alarm clears, the correlated alarms also clear. If a correlated alarm does not clear after the affected-object alarm clears, the source of the correlated alarm is an event other than the trigger event. In this case, the alarm correlation is removed and the alarm is displayed in the dynamic alarm list. See Procedure 37-9 for information about viewing correlated alarms.

You can enable or disable the display of correlated alarms in order to reduce the number of alarms that appear in the dynamic alarm list. Correlated alarms are displayed by default and can be enabled or disabled for individual 5620 SAM clients. See Procedure 37-7 for more information.

Note — The display of correlated alarms in the Alarm Window does not affect the alarm status displayed in the navigation tree and topology map.

You can configure the 5620 SAM to automatically delete correlated alarms when the correlating alarm is deleted. You can also configure 5620 SAM alarm settings to specify whether a user notification is displayed when one or more correlated alarms is about to be deleted. See Procedure 37-1 for information about configuring the automatic deletion of correlated alarms.

Note — A correlated alarm remains after the deletion of the correlating alarm if there is another correlating alarm associated with it. For this reason, the number of correlated alarms that are automatically deleted may be fewer than the number stated in the warning notification presented to a GUI operator.

Service and transport alarm correlation

The 5620 SAM provides limited service and transport alarm correlation. When an LSP goes out of service, the 5620 SAM raises an alarm against the LSP and raises a correlated alarm against each LSP path that is a child object of the LSP. The LSP alarm is listed as an aggregated alarm for each SDP that uses the LSP. A 5620 SAM operator can use the aggregated LSP alarm for SDP troubleshooting.

Because there is not necessarily a direct relationship between an LSP and the SDPs that use it, for example, when LDP over RSVP is the transport mechanism, the 5620 SAM does not correlate SDP alarms with LSP alarms.

Automatic purging of alarms

Large numbers of outstanding alarms can affect system performance. Therefore, outstanding alarms are purged based on the severity, correlation status, and age of the alarm. If the system limit of 60 000 is reached, alarms are purged to the historical alarm log until the alarm count drops to 45 000. Other automatic purging of alarms is not necessary when historical alarm logging and purging policies are configured, as described in Procedure 37-4.

The alarm purge algorithm sorts alarms based on the following criteria:

- correlated alarms are deleted before the root alarms are deleted
- lower severity alarms are deleted before higher severity alarms are deleted
- oldest alarms are deleted first

When alarm policies are not configured, the system purges alarms in this sequence:

1. When the outstanding alarm count reaches 50 000, non-critical and non-root alarms are purged to the historical alarm log until the alarm count drops to 45 000.
2. An alarm is raised to indicate an alarm purge is in process.
3. When the outstanding alarm count reaches 60 000, alarms are purged to the historical alarm log until the alarm count drops to 45 000.
4. An alarm is raised to indicate an alarm purge.

To ensure purged alarms are logged, you must set up historical alarm logging, as described in Procedure 37-4.

37.2 Workflow to manage alarms

1 Set up the managed NEs to send SNMP traps of managed NE faults and events to the 5620 SAM. See the appropriate NE documentation for more information.

2 Configure alarm policies on the 5620 SAM using Administration→Alarm Settings.

i Configure global policies for incoming alarms. See Procedure 37-1 for more information.

ii Configure specific policies for each alarm type. See Procedure 37-2 for more information.

iii Configure additional text policies. See Procedure 37-3 for more information.

iv Configure alarm history database behavior for the storage of historical alarm records. See Procedure 37-4 for more information.

3 Configure alarm user preferences. See Procedures 37-5, 37-6, and 37-7 for more information.

4 Monitor alarms:

i For SLAs by monitoring SAP and service alarms from the appropriate properties form or manage services form. See Procedure 37-8 for more information.

ii For each piece of equipment or logical component using the Faults tab button from each equipment form, logical component form, or from the navigation tree equipment view. See Procedure 37-9 for more information.

iii For the network from the dynamic alarm list. See Procedures 37-11, 37-12, 37-13, 37-14, 37-15, and 37-16 for more information.

iv For incoming SNMP traps from managed NEs by viewing logs.

For information about troubleshooting using alarms see the *5620 SAM Troubleshooting Guide*.

5 Review historical alarm records in the alarm history log database for trends and store the alarms for record-keeping. See Procedures 37-17 and 37-18 for more information.

6 View the object against which an alarm logged to the alarm history database was raised. See Procedure 37-19 for more information.

7 Reload alarms to ensure the alarm service cache is refreshed, as required by the system administrator. This step can only be performed by a user with an account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class, and should only be done when necessary. See Procedure 37-20 for more information.

37.3 Alarm management procedures

Use the following procedures to perform fault management tasks.

Procedure 37-1 To configure global alarm policies

Global alarm policies affect all network alarms and can be set by users who are assigned an account with either the administrator scope of command role or a scope of command role with write access permissions to the fm.GlobalPolicy class.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Alarm Behavior tab button.

3 Set the severity policies by clicking on the Severity tab button.

i Enable the Severity Alterable parameter to enable setting the severity parameters. When you enable severity alterable functionality, you can specify whether to allow automatic changes to severity based on individual alarm policies or manual changes to severity based on operator actions.

Severity settings cannot be altered unless the check box is enabled.

ii Configure the parameters.

- manual severity alterations
- severity promotion
- severity demotion
- clearing (if self-clearing alarm)
- automatic severity alterations
- implicit severity promotion
- implicit severity demotion
- escalation (defined by specific policy)
- De-escalation (defined by specific policy)

4 Set the deletion policies by clicking on the Deletion tab button:

i Enable the Alarm deletion parameter to allow the creation of a deletion policy.

Deletion policies cannot be changed unless the check box is enabled.

ii Choose the appropriate deletion policy. When you enable deletion functionality, you can specify whether to allow operators to delete alarms or allow the automatic deletion of alarms.

Configure the parameters.

- manual
- auto
- automatic deletion of correlated alarms

Caution — Deleting an alarm resets the frequency of an alarm to 1. This may cause conflicts with configured alarm escalation and de-escalation policies.

5 Click on the Apply button to save the changes. A dialog box appears.

6 Click on the Yes button to proceed.

7 Click on the Cancel button to close the form.

Procedure 37-2 To configure specific alarm policies

A specific alarm policy allows you to modify the behavior of a specific type of alarm, if you want that alarm to behave differently than the default.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens.

2 Click on the Specific tab button. A list of alarm types appears.

3 Choose an alarm type. Alternatively, you can select multiple alarms at the same time.

The alarm types are listed by *domain.alarm name*.

4 Click on the Properties button. The Specific Policy form for that alarm type opens.

5 Configure the general alarm type parameters.

- Group Tag
- Squelch
- Initial Severity Assignment
- Automatically Assigned Urgency
- Interval
- History Enabled

6 Configure the alarm type escalation parameters. Select the Escalation or De-escalation check boxes to escalate or de-escalate the severity of an alarm based on how frequently that alarm is processed by the 5620 SAM.

i Select the Escalation parameter or the De-escalation parameter.

ii Click on the Add button.

iii Configure the Frequency parameter. This is the threshold in a 24-hour period of how often the alarm must arrive before the severity is escalated or de-escalated.

The alarms are analyzed at faster, non-configurable intervals to verify whether the Frequency value is reached.

iv Configure the Severity parameter to specify the new severity applied against the alarm if the escalation or de-escalation threshold is reached.

v Click on the OK button.

The new escalation or de-escalation policy is applied to the alarm.

7 Click on the OK button to save the changes and close the Specific Policy form. A dialog box appears.

8 Click on the Yes button to proceed.

Procedure 37-3 To create additional text policies

Create an additional text policy to display specific information about an alarmed object in the additional text field of the dynamic alarm list and on the Alarm Info form.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Additional Text tab button.

3 Configure the additional text policies. Perform the following steps:

i Click on the Create button. The Additional Text Policy (Create) form opens with the General tab displayed.

ii Click on the Select button beside the Domain parameter. The Select affected object's domain form opens.

iii Select a domain from the list and click on the OK button. The Select affected object's domain form closes and the Additional Text Policy (Create) form reappears.

iv Click on the Select button beside the Object Type parameter. The Select affected object's object type form opens.

v Select an object type from the list and click on the OK button. The Select affected object's object type form closes and the Additional Text Policy (Create) form reappears.

vi Configure the parameters:

- Description
- Overwrite existing

4 Configure the additional text attributes. Perform the following steps:

   i Click on the Additional Text Attributes tab button.

   ii Click on the Create button. The Additional Text Attribute (Create) form opens.

   iii Click on the Select button beside the Attribute Name parameter. The Select affected object attribute form opens.

   iv Select an object attribute from the list and click on the OK button. The Select affected object attribute form closes and the Additional Text Attribute (Create) form reappears.

   v Configure the Order parameter.

   vi Click on the OK button. The Additional Text Attribute (Create) form closes and a dialog box appears.

   vii Click on the OK button to confirm the action.

   viii Click on the OK button to save the configuration. The Additional Text Policy (Create) form closes and the text policy appears in the list on the Alarm Settings form.

5 Close the form.

Procedure 37-4 To configure alarm history behavior

The 5620 SAM stores new and old alarms in the alarm history database for record-keeping and trend analysis. You can specify how alarms are stored in the database.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Alarm History DB Behavior tab button.

3 Set the alarm history behavior.

a Configure the parameters.

- Max 24hr Partition Log Size (records)
- Administrative State
- Log On Change
- Log On Deletion

Note — Alcatel-Lucent recommends enabling the Log on Deletion parameter to ensure historical log records of all deleted alarms exists.

b Purge alarms from the historical alarm database by clicking on the More Actions button and choosing Purge All or Purge Range. The Purge Range option can be used when a filter policy is applied by choosing the Set Purge Range option.

Caution — Using the Purge All option removes all alarm history records from the historical alarm database.

i Click on the More Actions button and choose Set Purge Range. The Alarms Settings Filter form appears.

ii Specify a filter that to be used as the purge criteria. For example, to purge the alarm history database of all minor alarms, set the Severity filter to equal minor.

iii Click on the OK button. The Alarms Settings Filter form closes.

iv Click on the More Actions button and choose Purge Range.

v A dialog box appears. Click on the Yes button to proceed.

The historical alarm database is purged of those alarm history records which met the purge criteria.

When the maximum number of alarms allowed in the alarm history database is reached, the oldest alarms are deleted. If you want to save information about those alarms, save a file containing the alarm log information, as described in Procedure 37-18.

Procedure 37-5 To configure audible alarms

1. Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
2. Configure the Turn on Audible Alarms parameter.
3. Click on the OK button. The User Preferences form closes, and the audible alarm option is applied.

Procedure 37-6 To configure alarm flags

The Monitoring Flag panel under the Alarm Table tab indicates the number of alarms, color-coded by severity, that have been detected since the flag was reset. The time the last alarm for that severity was detected is also displayed. You can show or hide alarm flags the Monitoring Flag panel using the User Preferences form.

1. Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
2. Configure the Show Alarm Flags parameter.
3. Click on the OK button. The User Preferences form closes, and the Monitoring Flag panel appears in the dynamic alarm list Alarm Window.

Procedure 37-7 To enable or disable the display of correlated alarms

Note 1 — The display of correlated alarms may slow GUI performance while the 5620 SAM adds the alarms to the dynamic alarm list.

Note 2 — When you disable the display of correlated alarms in the dynamic alarm list, the correlated alarms are still listed in the Correlated Alarms tab of the Alarm Info form.

Note 3 — You can configure the Show Correlated Alarms parameter on a per-session basis. The display of correlated alarms is automatically updated by the Show Correlated Alarms by Default parameter when the 5620 SAM client application loads.

1 Enable or disable the default display of correlated alarms in the alarms window. Perform the following steps.

- **i** Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
- **ii** Configure the Show Correlated Alarms by Default parameter.
- **iii** Click on the OK button. The User Preferences form closes and the display of correlated alarms in the Alarms Window is updated.

2 Enable or disable the display of correlated alarms in the Alarm Window. Perform the following steps.

- **i** Choose Application→Alarm Window from the 5620 SAM main menu, if required. The Alarm Window is displayed.
- **ii** Configure the Show Correlated Alarms parameter. Correlated alarms are displayed in the Alarm Window.

Note — The Alarm Window title bar displays Correlated Alarms Not Shown when correlated alarm display is disabled.

Procedure 37-8 To view alarms raised against equipment, logical components, and services

Alarms raised against network objects allow you to view faults on each NE in the network down to the service, path, or port level. The 5620 SAM analyzes all incoming alarms to ensure that the alarms are listed against the appropriate equipment or service. This feature is useful when you troubleshoot an equipment or service problem.

Objects that can have alarms issued against them contain a Faults tab button. The tables in the Faults tab button list the alarms issued against the specific equipment or service. For some forms, the Faults tab is further broken down into the Object Alarms, Affecting Alarms, Aggregated Alarms, and Alarms on Related Objects tabs. These tabs show alarms against specific objects, such as ports, and related problems, such as services that use the ports.

1 Choose a menu that displays a path, logical component or service form. For example:

  a Choose Manage→Equipment→Equipment. The Manage Equipment form opens.

  b Choose an NE from the drop-down list and click on the Properties button. The Network Element (Edit) form opens.

2 Click on the Faults tab button. A list of alarms appears under the appropriate tabs. Click on an appropriate tab button to display alarms of interest.

3 Review the alarm information. See Table 37-3 for the type of information available in an alarm. Scroll across each line to view the information contained in the alarm.

4 To view a specific alarm, double-click on the line or click on the View Alarm button to open the Alarm Info form. See Table 37-3 for the alarm information available under all tabs in the form.

5 Click on the View Alarmed Object button to open the properties form for the alarmed object.

6 Handle alarms according to your fault management policies. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Procedure 37-9 To view alarm information

Alarm information is available from:

- the dynamic alarm list
- the navigation tree
- policy, service, and other properties form Fault tabs
- the Manage Services and service properties forms, to use in conjunction with the service ID to determine which customer is affected by which service alarms
- the Alarm Info form that opens when you double-click on a row in the alarm list

You must ensure that you are on the correct form to view alarms. For example, you cannot view ping management connection alarms from the Discovery Manager configuration form even through that is the form on which you perform the pings, or the NE discovery control form, even though that is the form on which you choose the ping policy. You must navigate to the appropriate object form to find the alarms, which, in this example, is an NE properties form.

1 Click on the Faults tab button of an NE properties form to list the alarms.

2 Click on the appropriate fault tab button.

The fault tabs contain other tabs that list alarms against the specific object, alarms on objects that are directly affecting the object, aggregated alarms, and alarms against related objects that affect the specific object.

3 Open a listed alarm by selecting the alarm entry and clicking on the View Alarm button. Alternatively, you can double-click on the alarm entry.

Note — When sorting alarms, sorting more than 15 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms. Creating search filters for network alarms is described in Procedure 37-12.

4 Review the alarm information.

a View the alarm information in each tab and respond according to your alarm-handling policies.

Table 37-3 lists the types of alarm information available to users from the Alarm Info form. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Table 37-3 Alarm Info form fields

Field	Information
Alarm tab on Alarm Info form, Info tab displayed	
Domain	The general area of the 5620 SAM software that is affected by the alarm. This is of specific interest and use to those monitoring alarms using the XML OSS interface. See the *5620 SAM XML OSS Interface Developer Guide* for more information.
Application domain	
Site ID	IP address of the NE that raises the alarm
Site Name	Name of the NE
Object Type	Type of object
Alarmed Object Type	
Object Name	Name of the object
Alarmed Object Name	
Object Id	Unique string identifying the object down to the lowest level, for example, network ID #, chassis #, slot #, daughterCardSlot #
Alarmed Object Id	

(1 of 3)

Field	Information
Alarm	Name of the alarm
Alarm Name	
Time Detected	When the alarm was raised
Type	Vendor-specific and X.733 standards for the event type of the alarm
Alarm Type	
Severity	Vendor-specific, TMN, and X.733 standards for severity of the alarm
Alarm Severity	
OLC State	Configured OLC state
Cause	Vendor-specific and X.733 standards for the probable cause of the alarm
Probable Cause	
Ack	Whether the alarm has been acknowledged by an operator (true) or not (false)
Acknowledged	
Acknowledged By	Name of operator that acknowledged the alarm
Cleared By	Name of operator that last cleared the alarm
Urgency	Urgency setting of the alarm
Additional text	Any extra text included with the alarm
First Time Detected	Time of the first recorded instance of the alarm
Last Time Detected	Time of the last recorded instance of the alarm. This field provides useful information when multiple instances of the same alarm are raised. As each new instance of the alarm is raised, the number of occurrences statistic increases, and Last Time Detected shows the time that the last instance of the alarm was raised.
Number of correlated alarms	Number of correlated alarms
Correlating Alarm ID	Unique string that identifies the correlating alarm object down to the lowest level
Alarm tab on Alarm Info form, Severity tab displayed	
Severity details Cleared details Promoted details Escalated details	Information about alarm severity. You can modify the alarm severity by clicking on the View Policy button. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Alarm tab on Alarm Info form, Statistics tab displayed	
Frequency Number of Occurrences Number of Occurrences Since Clear Number of Occurrences Since Acknowledged	You can modify the alarm frequency by clicking on the View Policy button and modifying the individual alarm settings. How often the alarm has been raised, based on the specified scenarios. As each new instance of the alarm is raised, the number of occurrences statistic increases, and the Last Time Detected field shows the time that the last instance of the alarm was raised. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.

(2 of 3)

Field	Information
Acknowledgement tab on Alarm Info form, Acknowledgement Info tab displayed	
Acknowledged Acknowledged by Last Time Acknowledged Previously Acknowledged Assigned Urgency Urgency Assigned By	Information about when the alarm was acknowledged, the user that acknowledged the alarm, and the user that set the urgency. You can modify the acknowledgement and urgency by clicking on the View Policy button and modifying the individual alarm settings. The Previously Acknowledged parameter specifies that the alarm had been previously acknowledged. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Acknowledgement tab on Alarm Info form, Notes tab displayed	
View button Properties button New button Note tab button Revision History tab button	Create notes by clicking on the New button and entering the note. You can edit or view notes from the same form. Information about the note, including the time created and the name of the user who created the note, are displayed in rows for each note entered. Click on the Revision History tab button to view all notes created for the alarm. Select a note from the list and click on the View button to view the note.
Alarm tab on Alarm Info form, Details tab displayed	
Description Raising Condition Clearing Condition	A description of the alarm. Raising condition for the alarm. Clearing condition for the alarm.
Affected Objects tab on Alarm Info form	
Search button Properties button	Lists the objects that are affected by the alarm. Choose an affected object from the list and click on the Properties button to open the properties form for the object.
Affecting Objects tab on Alarm Info form	
Search button Properties button	Lists the objects that directly affect the object in alarm. Choose an affecting object from the list and click on the Properties button to open the properties form for the object.
Correlated Alarms tab on Alarm Info form	
Search button Properties button	Lists the objects that directly affect the object in alarm. Choose a correlated alarm from the list and click on the Properties button to open the Alarm Info form for the correlated alarm.

(3 of 3)

b Click on the Affected Objects tab button to view other network objects that are affected by this alarm. Choose an object and click on the Show Object(s) button to open the properties form for the affected object.

For example, a service tunnel alarm is raised. From the Alarm Info form, click on the View Alarmed Object button to go directly to the properties form for that service tunnel. The properties form opens. Click on the Faults tab button to see the same alarm listed under the Object Alarms tab button.

c Click on the Affecting Objects tab button to view other network objects that affect this object. Choose an object and click on the Show Object(s) button to open the properties form for the affecting object.

d Click on the Correlated Alarms tab button to view correlated alarms. Choose an alarm and click on the Show Alarm(s) button to open the Alarm Info form.

5 Handle the alarm according to your alarm-handling policy.

a Click on the Delete button to delete the alarm, if you have permissions to delete alarms. Click on the Yes button to confirm the action, and then click on the OK button.

Caution — You cannot recover a deleted alarm, unless deleted alarms are configured to be logged in the alarm history database, as described in Procedure 37-4.

b Click on the Clear button to clear the alarm. Click on the Yes button to confirm the action, and then click on the OK button. The alarm is cleared from the list, and is added to the alarm log as an alarm history record, if configured.

Note — Some alarms are self-clearing, which means that they are automatically cleared from the alarm list after the condition that triggered the alarm is no longer present. The dynamic alarm list contains an Implicitly Cleared attribute that identifies the self-clearing alarms.

c Click on the Acknowledge button to acknowledge the alarm.

i From the Notes tab, modify the urgency and assigned severity of the alarm, if required. You need permissions to modify the alarm.

ii From the Notes tab, add a note to the alarm, if required.

You can also choose a note from the list, click on the Properties button, and modify the note by setting the Reason for change and Detailed Text parameters.

iii Click on the Apply button to save the changes and acknowledge the alarm. If you added a note, the note appears in the list of notes.

When you view the alarm again, the acknowledgement information is updated to include:

- the user that acknowledged the alarm
- when the alarm was acknowledged
- whether the alarm had already been previously acknowledged
- any changes to the assigned urgency of the alarm

iv If required, you can click on the Revision History tab button and view a revised note. The revised note information includes:

- date modified
- user that modified the note
- reason for the note change
- an explanation of the note change
- contents of the note before and after the modification

d Click on the View Policy button. The Specific Policy form opens for that alarm type. You can view the policy configured for the alarm type, as described in Procedure 37-2.

e Click on the View Alarm History button to view the alarm history for this type of alarm. An Alarm History form appears with the Alarm Name filter equal to the type of alarm you are viewing.

i Click on the Search button. A list of alarm history records appears based on the filter.

ii Choose the record from the alarm history database log, as described in Procedure 37-17.

Procedure 37-10 To copy alarm information to a buffer

The alarm information copied to the local clipboard buffer can be pasted in other applications. This function helps you share the alarm information for troubleshooting purposes.

1 Click on the Faults tab button of an NE properties form to list the alarms.

2 Click on the appropriate fault tab button.

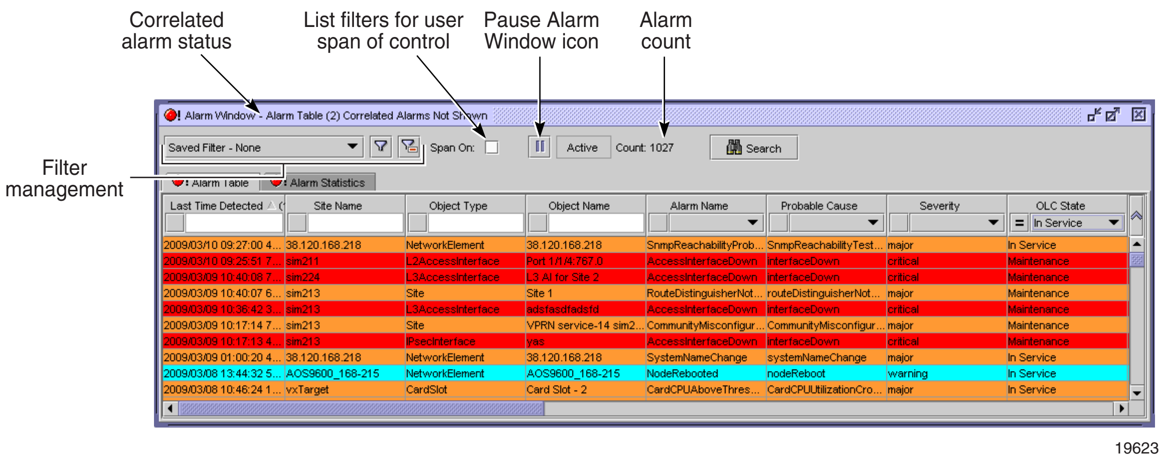
3 Open a listed alarm by selecting the alarm entry and clicking on the View Alarm button. Alternatively, you can double-click on the alarm entry.

4 Click on the Copy to Clipboard button. You can also use the contextual menu in the Alarm Window to copy the alarm information to the clipboard.

Procedure 37-11 To view all network alarms using the dynamic alarm list

The dynamic alarm list Alarm Window allows you to monitor incoming faults from the NEs and 5620 SAM software. This feature is most useful when monitoring the network. Figure 37-9 shows the dynamic alarm list Alarm Window.

Figure 37-9 Dynamic alarm list Alarm Window



1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

Note — You can open and view up to six alarm windows. This is useful when you need to view multiple filtered incoming network alarms.

2 Filter the alarms, if required.

Note — Sorting more than 15 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms.

a Choose a filter from the Save Filter drop-down list.

b Create a filter. See Procedure 37-12 for more information.

c Choose an OLC filter from the OLC Filter drop-down menu.

d Choose a severity filter from the Severity Filter drop-down menu.

3 Right-click on one or more alarms in the list. The contextual menu appears.

4 Choose:

a Show Alarm(s) to view the Alarm Info form for each selected alarm. Table 37-3 lists the alarm information displayed.

b Show Affected Object to display the configuration or property form for the object or objects against which the alarm or alarms is raised.

c Acknowledge Alarm(s) to open the alarm acknowledgement form for the alarm or alarms. Enter acknowledgement text, if required, and click on the OK button. Confirm the action. The acknowledgement information is added to the alarm info form, and any acknowledgement text is added to the Notes tab. The Acknowledged By column in the Alarm table indicates the user who acknowledges the alarm.

d Assign Severity to change the severity policy of the alarm using the Assigned Severity parameter. Click on the OK button. Confirm the action.

e Assign the OLC State to the alarm.

f Delete Alarm(s) to delete an alarm or alarms. Confirm the action to delete the alarm or alarms. The alarm or alarms are deleted and added to the alarm history database log as an alarm history record, if configured.

Caution — You cannot recover a deleted alarm, unless the alarm is configured to be logged on deletion, as described in Procedure 37-4.

g Clear Alarm(s) to clear the alarm or alarms. Confirm the action to clear the alarm or alarms. The alarm or alarms are cleared and added to the alarm history database log as an alarm history record, if configured.

h NE Sessions→*option* to start a SSH or Telnet session with the managed equipment that generated the alarm.

i Show Sorting to determine the sort order of how alarm information is displayed:

i Use the left, right, up, and down arrows to resequence the alarm fields as required.

ii Click on the Sort Ascending and Sort Descending buttons to specify the order of displayed alarms.

iii Click on the Close button to return to the dynamic alarm list.

j Copy to Clipboard to copy the alarm information to the clipboard buffer.

5 Handle the alarm(s) according to your fault management policies. Alarm handling is described in Procedure 37-9. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Procedure 37-12 To create search filters for network alarms

You can create and select filters to view specific network alarms in the dynamic alarm list. You can save multiple filters and view the alarm information by opening up to 6 alarm windows. The name of the filter appears in the alarm window title of each alarm window that is open. Viewing network alarms using the dynamic alarm list is described in Procedure 37-11. Figure 37-9 shows the location of the Manage Filters icon in the alarm window.

Note — The FDN extension of a generic NE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for generic NE alarms that have FDN extensions, you must filter on the Additional Text field.

1 Choose Application→Alarm Window. The Alarm Window opens.

2 Click on the Filter icon beside the filter drop-down list. The Alarm Window filter form opens.

3 Configure the filter criteria.

4 Click on the Add button. The Save Filter form opens.

5 Click on the Save button. The Save Filter form opens.

6 Configure the parameters:

- Filter Name
- Description
- Public

7 Click on the Save button. The Save Filter form closes and the Alarm Window filter form reappears.

8 Close the Alarm Window filter form.

9 Click on the filter drop-down list. The saved filter is shown in the list.

10 Click on the saved filter to load and view the results of the filtered search in the dynamic alarm list. The number of alarms associated with the selected search filter appears in the Count field, as shown in Figure 37-9.

Procedure 37-13 To change the severity filter from the alarm window

1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

2 If required, click on the filter icon to create a filtered list of alarms. See chapter 3 for more information about creating search filters.

3 Right-click on the alarm, a drop down menu appears.

4 Choose Assign Severity. A Severity Assignment window opens.

5 Choose one of the following options. The alarm table panel is refreshed with a filtered list of alarms.

- Severity Filter - None
- cleared
- indeterminate
- info
- condition
- warning
- minor
- major
- critical

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Severity Assignment window closes.

Procedure 37-14 To pause the dynamic alarm listing

New incoming alarms are added to the dynamic alarm list, with the most recent alarm shown first. If you are viewing an alarm from the dynamic alarm list, new incoming alarms may cause the alarm list to scroll automatically. You can pause the dynamic alarm list to prevent this. Figure 37-9 shows the location of the Pause Alarm Window icon in the Alarm Window.

1 View alarms from the dynamic alarm list, as described in Procedure 37-11.

2 Click on the Pause Alarm Window icon. The icon changes to indicate that the dynamic alarm list Alarm Window is locked for viewing. The icon box changes to red and the text changes to Paused.

Incoming alarms are not added for the duration of the pause.

3 Click on the Pause Alarm Window icon to unlock the dynamic alarm list Alarm Window. The icon changes to indicate the dynamic alarm list Alarm Window is active. The icon box changes to gray and the text changes to Active. Any alarms that occurred during the pause appear in the dynamic alarm list.

Note — You can also scroll lock the dynamic alarm list by highlighting a specific alarm. New incoming alarms appear above the selected alarm, but the selected alarm continues to be selected in the dynamic alarm list. Use the down scroll bar to find the selected alarm.

Procedure 37-15 To view network alarm statistics

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Click on the Alarm Statistics tab button in the Alarm window. The alarm statistics table appears.

2 View the alarm statistics information.

The Alarm Statistics table lists the number of network alarms sorted in columns by acknowledged and unacknowledged status, and then by the number of critical, major, minor, warning, condition, info, indeterminate, and cleared alarms.

Procedure 37-16 To view current and historical alarms

Use this procedure to view current and historical alarms for a given time period. This consolidated view of all relevant alarms will facilitate troubleshooting.

1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

2 Select one or more alarms in the list.

3 Click on the Historical Alarms button and choose Current and Historical Alarms Snapshot. The Current and Historical Alarms Snapshot form opens, displaying current and historical alarms for the time period specified by the First Time Detected (minus buffer time) and Last Time Detected (plus buffer time) of the selected alarms.

4 If required, modify the Display Buffer Time (minutes) parameter.

5 Double-click on an alarm in the list to view alarm information, as described in Procedure 37-9.

6 Close the Current and Historical Alarms Snapshot form.

Procedure 37-17 To review historical alarm records

Alarms are logged as historical alarm records in an alarm log database.

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, specify a filter to narrow the range of historical alarms displayed.

> **Note —** When sorting alarms, sorting more than 50 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms. Creating search filters for network alarms is described in Procedure 37-12.

3 Click on the Search button. The list of historical alarm records appears based on the filtering criteria.

4 Select an alarm history record from the list.

5 Click on the Properties button to review the alarm. The alarm history object form appears.

Table 37-3 lists the information displayed for each historical alarm record. Table 37-4 lists the additional historical alarm information available from the alarm history form for logged alarms.

Table 37-4 Alarm information from the Alarm History Object form

Alarm field	Information
Info tab on Alarm History Object form	
Alarm Status	Reason the alarm was logged to the historical alarm database
Last Time Acknowledged	Last time the alarm was acknowledged
Deleted By	Name of operator that deleted the alarm
Time Logged	Timestamp when alarm was moved to the historical alarm database
Highest Severity	The most severe status assigned to the alarm. Alarm severity can change due to escalation policies
Number Of Occurrences	How often the alarm was raised
Severity tab on Alarm History Object form	
Detected details Urgency details	Information about the alarm severity

6 Manage the logged historical alarm records.

i Click on the Cancel button to close the Alarm History Object form. The Alarm History form reappears.

ii Choose an alarm history record from the list.

iii Click on the Properties button. The AlarmHistoryObject form opens.

iv Click on the View Policy button to view the Specific Policy form. See Procedure 37-2 for more information.

v Click on the Purge Filtered button to purge alarms that meet the purging criteria. Click on the Yes button to confirm the action.

Caution — You cannot recover alarms purged from the historical alarm database log. If you want to save information about those alarms, save a file containing the alarm history database log details, as described in Procedure 37-18.

7 Close the Alarm History form.

When the maximum number of alarms allowed in the alarm log is reached, the oldest alarms are deleted. If you want to save information about those alarms, save a file containing the alarm log details, as described in Procedure 37-18.

Procedure 37-18 To save lists of logged historical alarm records

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The list of logged historical alarm records appears.

4 Sort the list of logged historical alarm records, as required.

5 Right-click on a list column heading and choose Save To File from the contextual menu. The Save form opens.

6 Save the list according to your company practices. You can:

- choose a directory to save the listed information using the Save In parameter
- create a filename of any length using the File Name parameter
- choose a format for the output file: HTML or comma-delimited CSV

7 Click on the Save button. The information is saved in the appropriate file format.

Procedure 37-19 To view the object against which an alarm logged to the alarm history database was raised

You can view the object that was the source of the historical alarm.

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The historical alarm records appear based on the filtering criteria.

4 Double-click on an alarm in the list. The alarm history record opens.

5 Click on the View Alarmed Object button. The configuration form, properties form, or other appropriate form opens. This is the form for the object that was the source of the original alarm.

Procedure 37-20 To reload all alarms

The 5620 SAM uses an alarm service to cache alarm information. To ensure the cache is current with all alarms stored in the database, administrators can reload all alarms from the database.

Caution — After the procedure is complete, client GUI users viewing open alarm forms and windows may have out-of-date information. Operators should close all open windows and forms, then relaunch them. This includes windows and forms displaying alarm status information, for example, the navigation tree.

1 Log in to a 5620 SAM client GUI with a user account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class. Enter and confirm the password and click on the OK button.

2 Choose Administration→Reload Alarm Information from the 5620 SAM main menu.

3 Clicking on the OK button to confirm that you are aware of all of the other users that will be affected by the alarm reload.

Alarm information is reloaded, and all active client GUIs are updated with the confirmation message that the alarms have been reloaded. Client GUI users can close then reopen windows as required, to refresh the alarm information.

4 Click on the OK button to confirm the message.

5 Close then reopen any open windows or forms, if required.

Procedure 37-21 To perform a 9500 MPR error recovery

This procedure applies to cleaning up inconsistencies created due to MIB population failures which can occur during service creation on 9500 MPR NEs. Inconsistencies on these NEs can be detected during full NE synchronization or on opening the NE properties form. The user will be notified by an implicitly cleared alarm with a Warning severity level on the NE.

1 Right-click on a 9500 MPR NE instance, and select Properties from the drop-down menu. A Network Element (Edit) form opens.

2 If there are NE inconsistencies, a Cleanup Inconsistencies option will appear under the More Actions button.

3 Click on the More Actions button and choose Cleanup Inconsistencies.

4 Click on the Faults tab button of the Network Element (Edit) form to check for any remaining NE inconsistency alarms.

Note — For failures during 9500 MPR service creation the user should, after clearing the deployer, perform the following:

- A full resynch of the NEs on which service creation failure has occurred in order to restore existing NE entries
- Perform Procedure "To perform a 9500 MPR error recovery" to clean up inconsistencies.
- Complete the service by clicking on the Complete Service button.
- It is recommended that the inconsistencies be cleaned up prior to any new service creation.

38 — OAM diagnostic tests

38.1 OAM diagnostic tests overview

The proper delivery of services requires that a number of operations must occur correctly at different levels in the service. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel, must be performed successfully for the service to pass traffic to subscribers as agreed to according to SLAs.

Even when tunnels are operating correctly and are correctly bound to services, incorrect information may cause connectivity issues.

To verify that a service is operational and that configuration information is correct, a set of configurable in-band or out-of-band, packet-based OAM tools is available.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the forwarding path. However, these packets are distinguishable from customer packets, so they are kept within the service provider network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across a portion of the transport network, for example, across LSPs to test reachability.

You can configure and manage OAM tests:

- from the properties forms of network objects, for example, LSP pings from the LSP properties form
- from the Manage Tests form
- from the service and composite service flat topology maps

You can create and schedule the execution of test suites that contain groups of OAM tests using the 5620 SAM Service Test Manager, or STM. See chapter 78 for information about the STM. See chapter 79 for information about scheduled tasks. See chapter 5 for information about managing tests and test results using service flat topology maps.

Table 38-1 lists the supported OAM test types, the objects against which the tests can be performed, the test types, and the network layer being tested.

Table 38-1 OAM test types and test objects

Network level	Test type	Network object or service component for test
Application (level 7)	DNS lookup	DNS
	DHCP lookup [2]	DHCP

(1 of 3)

Network level	Test type	Network object or service component for test
Ethernet	CFM Loopback	Ports
	CFM Global MEG	
	CFM Link trace	
	CFM Continuity Check	
	CFM One Way Delay	
	CFM Two Way Delay	
	CFM Eth test	
	CFM Single Ended Loss	
	CFM Two Way Synthetic Loss Measurement (SLM)	
Service (level 6)	VPRN ping	VPRN site
	VPRN trace	
	ICMP ping	
	ICMP trace	
	CPE ping	VPLS site Epipe VLL site
	MFIB ping	
	ANCP loopback	Network element
	VCCV ping	VLL
	VCCV trace	VLL
	MAC populate	VPLS site Epipe VLL site VLL MEF MAC Ping is only supported on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0 VPLS sites.
	MAC ping	
	MAC trace	
	MAC purge	
	MEF MAC ping[1]	
Service transport binding (level 5)	Service site ping	Network element
Service transport (level 4)	MTU ping	Service tunnel (SDP)
	SDP ping	
Transport (level 3)	LSP ping	LSP LSP path
	LSP trace	
	P2MP LSP ping	P2MP LSP P2MP path
	P2MP LSP trace	
	LDP ping [2]	MPLS site LDP site
	LDP trace [2]	
	LDP tree trace	

(2 of 3)

Network level	Test type	Network object or service component for test
Routed network (level 2)	ICMP ping	IP unicast traffic
	ICMP traceroute	
	OmniSwitch ping and traceroute[4]	
	Multicast trace	IP multicast traffic
	Multicast stat [3]	
	Multicast router information	
Layer 1 or Layer 2 (level 1)	MAC ping [3]	Ethernet
	MAC traceroute [3]	
	ATM ping	ATM PVC connection

(3 of 3)

Notes

(1) Supported only on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0.

(2) Cannot be performed using the 5620 SAM or using CLI on devices.

(3) Not yet supported using the 5620 SAM but is supported using CLI on devices.

(4) Implemented using user-defined scripts

Ethernet CFM

Ethernet Connectivity Fault Management (CFM) supports end-to-end service management in an L2 network. CFM tools provide path discovery and fault detection, isolation, and notification. See chapter 46 for more information about how to configure an IEEE 802.1ag-enabled network for Ethernet CFM.

The following CFM diagnostic tests detect connectivity failure.

CFM continuity check

CFM continuity check, or CC, messages, are multicast messages that a MEP transmits periodically to remote MEPs in the same MEG. CC tests are used to discover a remote end point, check the health of a site, and detect cross-connect misconfigurations. The loss of three consecutive CCM messages, or the receipt of a CCM with incorrect information, indicates a fault.

Note 1 — If a service is modified after you associate it with an MD, for example, a new site is added, you must manually add new MEPs, as required.

Note 2 — If a CFM continuity check test is running on a service when you add a new MEP to the service, you must stop the test and execute it again to make the new MEP active.

Note 3 — When a service is modified after a CFM continuity check is created, for example, a new B-VPLS site is added to the service, you must manually add a virtual MEP to the site.

CFM dual-ended loss

A CFM dual-ended loss test functions as an optional extension of a CC test. It applies only to Y.1731 MEPs. This type of test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between two MEPs. When a CC test is executed with the dual-ended loss option enabled, the option is replicated on all participating MEPs that support the test, along with the accompanying alarm threshold values. If a MEP detects that the local or remote frame loss ratio has exceeded the alarm threshold for a remote MEP, the MEP raises an alarm against the remote MEP.

CFM single-ended loss

The CFM single-ended loss test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a single-ended loss test is a destination MAC address. The test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between the two MEPs.

CFM loopback

CFM loopback messages are sent to a unicast destination MAC address. The MEP at the destination responds to the loopback message with a loopback reply. A MEP or a MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. CFM loopback tests verify connectivity to a specific MEP or MIP.

CFM link trace

CFM link trace messages that contain a target unicast MAC address are sent to multicast destination MAC addresses. Each MIP at the same MD level replies with a link trace response. Messages are forwarded to the next hop until they reach the destination MAC address. The originating MEP collects the replies to determine the path.

CFM one-way delay

The CFM one-way delay test applies only to Y.1731 MEPs. The test originates on one MEP and terminates on a target MEP. The results are read from the target MEP. In the test, frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source site until the frame is received by the destination site. The frame delay represents the one-way trip time between the source and destination sites.

CFM two-way delay

The CFM two-way delay test applies only to Y.1731 MEPs. In this test, the frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by the source site until the frame is received by the same site after passing through the destination site. The frame delay represents the round-trip time between the source and destination sites.

CFM Eth

The CFM Eth test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a CFM Eth test is a MAC address. The test is used to perform one-way in-service diagnostics that include verifying bandwidth throughput, frame loss, and bit errors. To perform the test, a MEP inserts frames with Eth-test information that includes specific throughput, frame size, and transmission patterns. A MIP is transparent to Eth-test frames.

CFM two-way SLM

The CFM two-way SLM test provides Synthetic Loss Measurement and it is used to check the packet loss.

MTU ping OAM

The MTU Ping OAM diagnostic tool, which is called sdp-mtu in the CLI, provides a tool for service providers to determine the exact frame (MTU) size that is supported on a service tunnel (also called an SDP), to within one byte. Use the MTU ping OAM to:

- determine the maximum frame size supported between the service ingress and the service termination point
- solve troubleshooting issues that are related to equipment used across the network core that may not be able to handle large frame sizes

In a large network, network devices can support a variety of packet sizes, up to a limit, that are transmitted across its interfaces. This size limit is referred to as the MTU of network interfaces. You must consider the MTU of the entire service tunnel end-to-end when you provision services, especially for VLL services in which the service must support the ability to transmit the largest customer packet.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the MTU Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE’s system interface address was used for this purpose.

Tunnel ping OAM

The Tunnel Ping OAM tool, which is called sdp-ping in the CLI, performs in-band unidirectional or bidirectional connectivity tests on service tunnels (also called an SDP). The OAM packets are sent in-band in the tunnel encapsulation, so they follow the same path as the service traffic. The response can be received out-of-band in the control plane or in-band using the data plane for a bidirectional test.

For a unidirectional test, tunnel ping OAM tests:

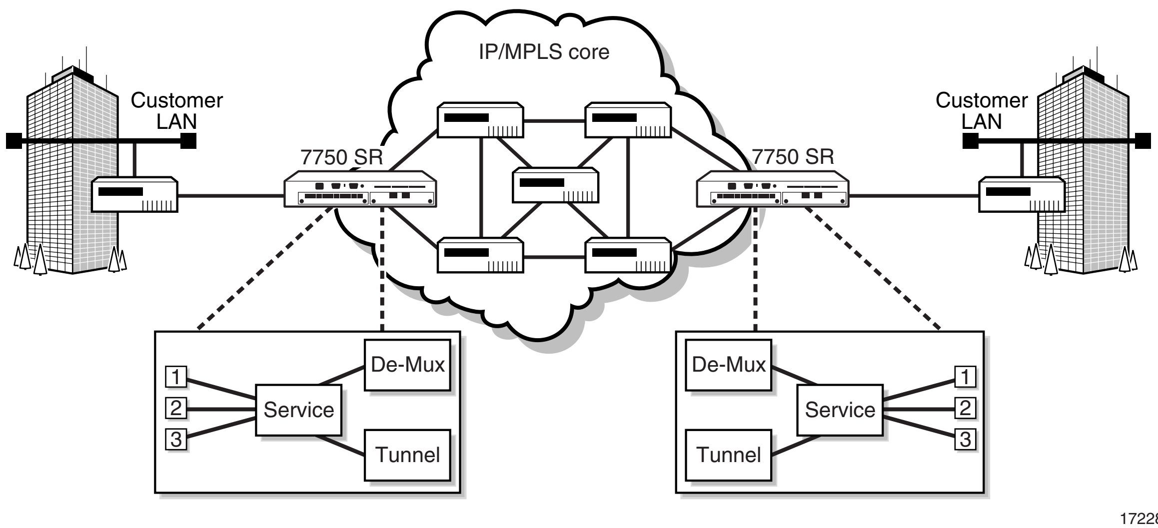
- egress service tunnel ID encapsulation
- whether the packet can reach the far-end IP address destination of the service tunnel ID within its encapsulation

- whether a packet of the specified size goes to the far-end IP address of the service tunnel ID within its encapsulation
- forwarding class mapping to ensure that the test packet is treated the same as the customer traffic
- determine whether SLA delay metrics are met

For a bidirectional test, tunnel OAM uses a local egress service tunnel ID and an expected remote service tunnel ID, so the user can specify where the returned messages should be sent from based on the far-end tunnel ID.

Figure 38-1 shows how a tunnel OAM packet can be inserted to test the connectivity between two customer LANs across the IP/MPLS core.

Figure 38-1 Sample OAM diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the Tunnel Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

Service site ping OAM

The Service Site Ping OAM diagnostic tool, which is called svc-ping in the CLI and was formerly called the circuit ping, provides end-to-end connectivity testing for an individual service. This diagnostic operates at a higher level than the tunnel OAM ping because it verifies connectivity for an individual service rather than connectivity across the service tunnel. This allows you to isolate a problem within the service rather than at the port, which is the endpoint of the service tunnel.

The diagnostic tests a service ID for correct and consistent provisioning between two service endpoints. The following information can be obtained from a service site ping OAM:

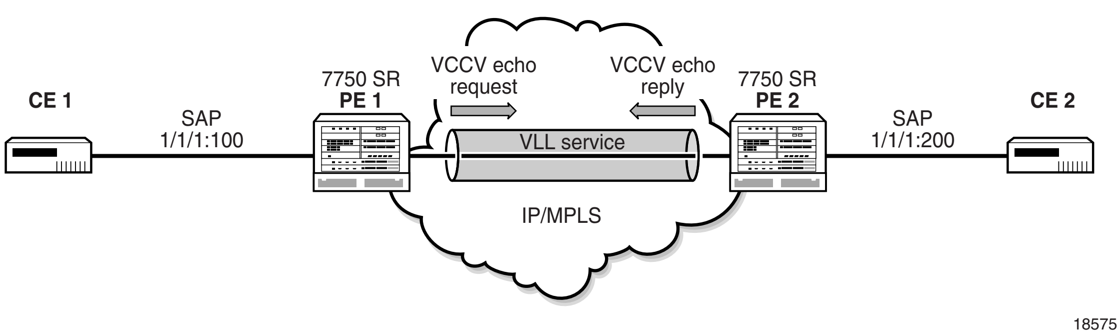
- verification that the local and remote service sites exists
- verification of the current state of the local and remote service sites
- ensuring that the local and remote service types are correlated
- ensuring that the same customer is associated with the local and remote service sites
- ensuring that there is a service-to-circuit association at both the local and remote service sites using the Use Local Tunnel and Use Remote Tunnel options, to check the circuit between service sites
- verification that the local and remote ingress and egress service labels match

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the Service Site Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

VCCV Ping OAM

The VCCV Ping OAM diagnostic tool, which is called vccv-ping in the CLI, performs in-band VLL connectivity tests. It can be used for all types of VLLs and supports cross-circuit tests as long as the circuit types match; for example, an epipe to epipe connector. The purpose of the ping is to determine that the destination PE device is the egress for the L2 FEC. Figure 38-2 shows a VCCV Ping.

Figure 38-2 VCCV Ping OAM diagnostic



In this example, the ping test packet or packets are sent with the destination IP address of PE 2. The request is encapsulated in a VLL packet and is forwarded to PE 2. PE 2 replies to the source device IP address. The packets are sent using the same encapsulation and along the same path as user packets in the VLL. This test provides a check of both the control plane and the data plane.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the VCCV Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

VCCV trace OAM

The VCCV Trace OAM diagnostic tool, which is called vccv-trace in the CLI, displays the hop-by-hop path used by the VLL. VCCV trace can trace the entire path of a PW with a single command issued at the T-PE or at an S-PE. It is an iterative process by which the ingress T-PE or T-PE sends successive VCCV-Ping messages with incrementing the TTL value, starting from TTL=1. The process is terminated when the reply is from the egress T-PE or when a timeout occurs.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the VCCV Trace OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

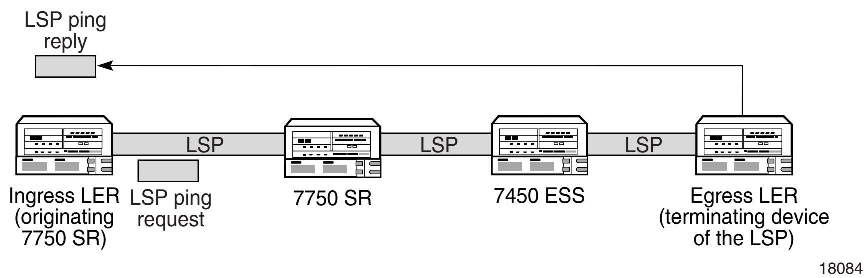
LSP Ping OAM

The LSP Ping OAM diagnostic tool, which is called lsp-ping in CLI, performs in-band LSP connectivity tests. The following information can be determined from the test:

- detect data plane failures in LSPs and with LSP connectivity
- test whether the LSP tunnels are working in both directions

In an LSP ping, the originating router creates an MPLS echo request packet for the LSP and MPLS path to be tested. The MPLS echo request packet is sent and awaits an MPLS echo reply packet from the router that terminates the LSP. The status of the LSP is displayed when the MPLS echo reply packet is received. Figure 38-3 shows an LSP ping.

Figure 38-3 LSP Ping diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LSP Ping use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

LSP Trace OAM

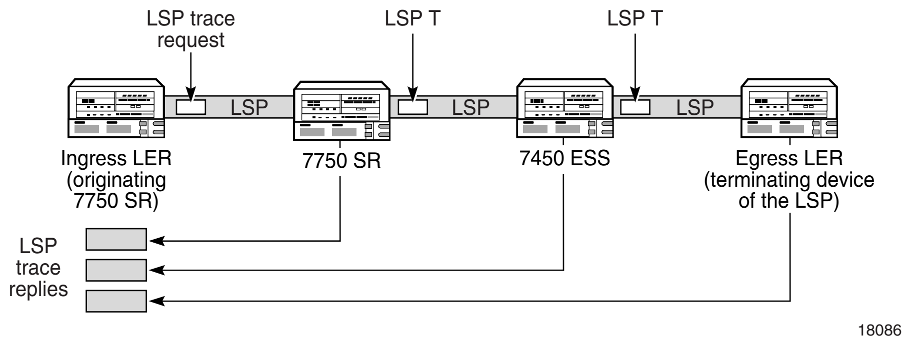
The LSP Trace OAM diagnostic tool, which is called lsp-trace in CLI, displays the hop-by-hop route used by the LSP. The following information can be determined from the test:

- hop-by-hop path for an LSP
- destination path of the packets

In an LSP trace, the originating router creates an MPLS echo request packet for the LSP to be tested. The packet contains increasing TTL values. The MPLS echo request packet is sent and awaits a TTL exceeded response or the MPLS echo reply packet from the router that terminates the LSP. The devices along the hop-by-hop route reply to the MPLS echo request packets with TTL and MPLS echo reply information.

Figure 38-4 shows an LSP trace.

Figure 38-4 LSP Trace diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LSP Trace use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

P2MP LSP Ping OAM

The PSMP LSP Ping OAM diagnostic tool, which is called p2mp-lsp-ping in CLI, performs in-band LSP connectivity tests.

The echo request message is sent on the active P2MP instance and is replicated in the data path over all branches of the P2MP LSP instance. By default, all egress LER nodes which are leaves of the P2MP LSP instance will reply to the echo request message.

You can reduce the scope of the echo reply messages by explicitly entering a list of addresses for the egress LER nodes that are required to reply. A maximum of 5 addresses can be specified in a single run of the p2mp-lsp-ping command. If all 5 egress LER nodes are 7x50 nodes, they will be able to parse the list of Egress LER addresses and will reply. The p2mp-lsp-ping command specifies that only the top address in the P2MP Egress Identifier TLV must be inspected by an egress LER. When interoperating with other implementations, an 7x50 egress LER will respond if its address is anywhere in the list. Furthermore, if another vendor implementation is the egress LER, only the egress LER matching the top address in the TLV may respond.

If you enter the same Egress LER address more than once in a single p2mp-lsp-ping command, the head-end node displays a response to a single one and displays a single error warning message for the duplicate ones. When queried over SNMP, the head-end node issues a single response trap and issues no trap for the duplicates.

P2MP LSP Trace OAM

The PSMP LSP Trace OAM diagnostic tool, which is called p2mp-lsp-trace in CLI, performs in-band LSP connectivity tests.

The LSP trace capability allows you to trace the path of a single S2L path of a P2MP LSP. Its operation is similar to that of the p2mp-lsp-ping command, but the sender of the echo reply request message includes the Downstream Mapping TLV to request the downstream branch information from a branch LSR or BUD LSR. The branch LSR or BUD LSR will then also include the Downstream Mapping TLV to report the information about the downstream branches of the P2MP LSP. An egress LER must not include this TLV in the echo response message.

The parameter probe-count operates in the same way as in the LSP Trace on a P2P LSP. It represents the maximum number of probes sent per TTL value before giving up on receiving the echo reply message. If a response is received from the traced node before reaching maximum number of probes, then no more probes are sent for the same TTL. The sender of the echo request then increments the TTL and uses the information it received in the Downstream Mapping TLV to start sending probes to the node downstream of the last node which replied. This continues until the egress LER for the traced S2L path replied.

LDP Tree Trace OAM

The LDP Tree Trace OAM diagnostic tool, which is called ldp-treetrace in OAM level of the CLI, is used to detect and discover the ECMP routing paths for a LSP between egress and ingress routers. The following information is determined from the test:

- number of ECMP paths
- number of failed hops

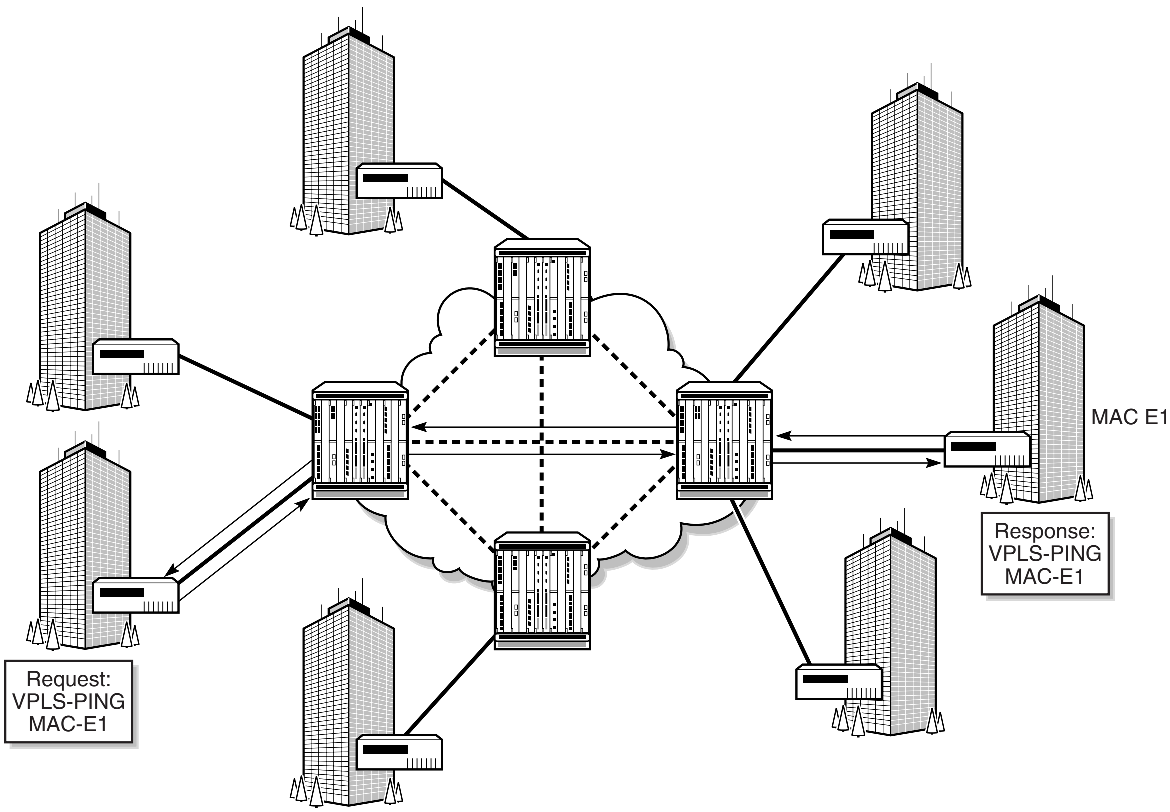
In an LDP tree trace, the originating router creates an MPLS echo request packet. The packet contains a set of IP header destination addresses. Routers along the path reply to the request with information about themselves and neighboring routers in the downstream path. The originating router uses this information to probe the downstream routers until it discovers a bit map setting common to all routers along the path. The result is a tree of available routers that the originating router can use for next hops. After discovery, the paths are tested using LSP ping and LSP trace.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The messages of the LDP Tree Trace use the T-LDP local LSR ID as the source IP address. Previously the NE’s system interface address was used for this purpose.

MAC ping OAM

The MAC ping OAM tool, which is called mac-ping in CLI, is used to test connectivity in a VLL or VPLS by verifying a remote MAC address at the far end of a service. Figure 38-5 shows a sample MAC ping from one end of a service to the far-end MAC address of the service.

Figure 38-5 Sample MAC ping diagnostic



The MAC ping determines the existence of the far-end egress point of the service. MAC pings can be sent in-band or out-of-band. You must specify either:

- the target (far-end) MAC address
- the broadcast address

In a MAC ping that is out-of-band, the ping is forwarded along the flooding domain when no MAC address bindings exist or is sent along the bindings if MAC address bindings exist. A response ping is sent from the far-end device when there is an egress binding for the service.

In a MAC ping that is in-band, the ping is sent with a VC label TTL of 255. The ping packet goes across each hop, and when it reaches the egress router, it is identified by the OAM label and the response is sent back along the management plane.

MEF MAC ping

Use the MEF MAC ping OAM tool to test connectivity in a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, VPLS site. The MEF MAC ping verifies a remote MAC address at the far end of the service.

MEF MAC ping must run simultaneously in both directions between the VPLS sites being tested.

MAC trace OAM

The MAC trace OAM tool, which is called mac-trace in CLI, displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end of a service. MAC traces can be sent in-band or out-of-band.

You must specify either:

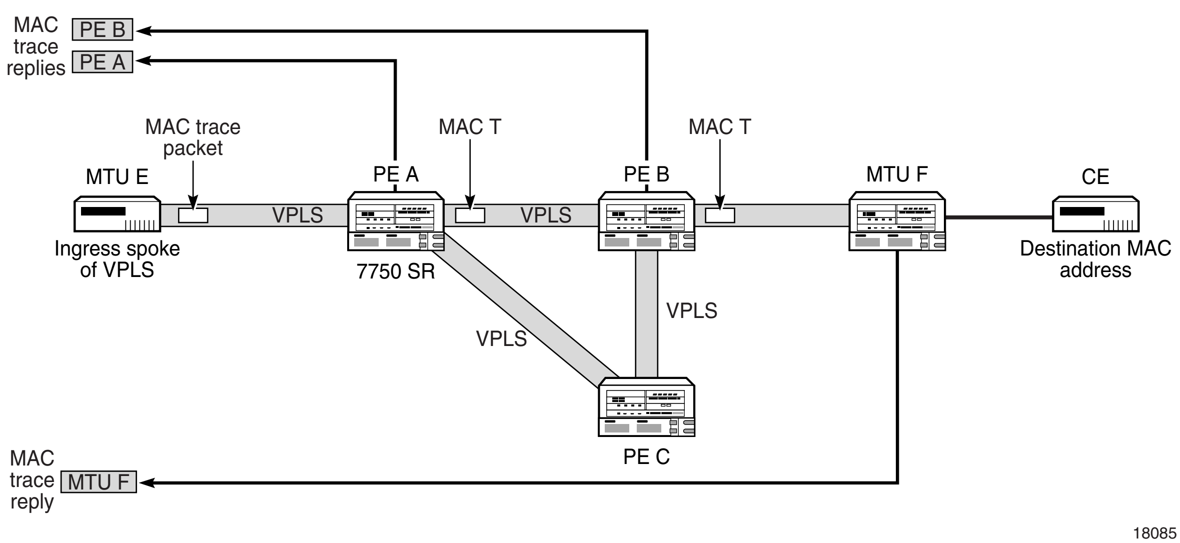
- the target (far-end) MAC address
- the broadcast address

In a MAC trace that is out-of-band, the destination IP address is specified by mapping the destination MAC address. If the destination MAC address is known to be a specific site, the far-end IP address of the service tunnel is used. If the destination MAC address is not known, the packet is sent to all service tunnels in the service.

In a MAC trace that is in-band, the trace request contains tunnel encapsulation, VC label, OAM, and other information. If the destination MAC address is known, the appropriate tunnel encapsulation and VC label is used. If the destination MAC address is not known, the packet is sent to all service tunnels, including all necessary tunnel encapsulation and egress VC labels for each bound service tunnel.

Figure 38-6 shows a MAC trace.

Figure 38-6 MAC trace diagnostic



MAC populate OAM

The MAC populate OAM tool, which is called mac-populate in CLI, is used to:

- Know whether the FIB table is accurate by testing forwarding plan correctness. This is done by populating a service FIB with an OAM-tagged MAC entry. This MAC entry indicates that the node is the egress node for the MAC address of a service. You can then use the FIB manager to see the OAM-tagged MAC entry.
- Send a message through the flooding domain to learn a MAC address, as if a customer packet with that source MAC address had flooded the domain from that ingress point of the service.

You can:

- force an existing MAC address to become OAM-tagged
- distinguish, in the FIB manager, MAC addresses that are OAM-tagged
- age an OAM-tagged MAC address

In a MAC populate, the OAM-tagged MAC address is populated on the egress point of the service. You can specify whether to flood this OAM-tagged MAC address to other devices so that the same OAM-tagged entry is added to the FIB tables of other devices.

MAC purge OAM

The MAC purge OAM tool, which is called mac-purge in CLI, is used to delete an OAM-tagged entry from a FIB, which was generated using the MAC populate OAM tool. This clears the FIB of any learned information for a specific MAC address, allows the FIB to be populated only by a MAC populate request, and can be used to flush all devices in a service domain.

CPE ping

The CPE ping tool, which is called cpe-ping in the CLI, is used to trace the end-to-end switching of specified MAC addresses of customer premises equipment. This ping extends the functionality of the MAC ping beyond the egress (customer-facing) port by allowing a ping to the SAP of a VPLS.

ANCP loopback

The ANCP loopback test, which is called oam ancp in the CLI, is used to send DSL OAM commands to complete an OAM test from a centralized point or when operational boundaries prevent direct access to the DSLAM. The ANCP loopback test raises an alarm that generates a log event displaying both successful and failed results.

VPRN ping and VPRN trace

The VPRN ping and VPRN trace OAM tools are enabled from the VRF site of the subscriber’s VPRN service. The VPRN ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. VPRN pings can be sent in-band or out-of-band.

The VPRN trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of customer traffic. VPRN traces can be sent in-band or out-of-band.

ATM OAM ping

The ATM OAM ping tool, which is called atmoam-ping in CLI, performs an ATM ping on an existing ATM PVC from the PVC endpoint using ATM OAM loopback cells. An ATM ping tests VC integrity and endpoint connectivity for PVCs using OAM loopback capabilities.

Multicast FIB ping

The multicast FIB ping OAM tool, which is called mfib-ping in CLI, identifies the SAPs that egress an IP multicast stream within a VPLS. This diagnostic can also be used to display the SAPs that are operationally up in the VPLS.

Multicast router information

The multicast router information OAM tool, which is called mrinfo in CLI, identifies VPRN multicast information for the target router. The information includes details that are related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

Multicast trace

The multicast trace OAM tool, which is called mtrace in CLI, identifies the hop-by-hop route used by VPRN multicast traffic to reach the target router. This diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. The 5620 SAM attempts to trace the receiver-to-sender route for the traffic. The destination of the diagnostic can be any PIM-enabled interface in the routing instance.

ICMP ping

The ICMP ping OAM tool, which is called icmp-ping in CLI, identifies the reachability of a remote host across the IP network. The tool is used with ICMP trace to detect and localize faults in IP networks.

The ICMP ping OAM tool can also be enabled from the VRF site of the subscriber's VPRN service. An ICMP ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. ICMP pings can be sent in-band or out-of-band.

ICMP trace

The ICMP trace OAM tool, which is called icmp-trace in CLI, identifies the diagnostic used to trace the ICMP traceroute control table. The tool is used with ICMP ping to detect and localize faults in IP networks.

ICMP trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of subscriber traffic. ICMP traces can be sent in-band or out-of-band.

OmniSwitch ping and traceroute

The 5620 SAM supports OmniSwitch ping and traceroute by using user-defined CLI scripts. See Procedure 38-38 for information about creating an OmniSwitch OAM script. See Procedures 38-40 and 38-41 for information about configuring and running OmniSwitch OAM scripts.

DNS ping

The DNS ping OAM tool, which is called dns-ping in CLI, identifies the diagnostic used to ping the DNS name, if DNS name resolution is configured.

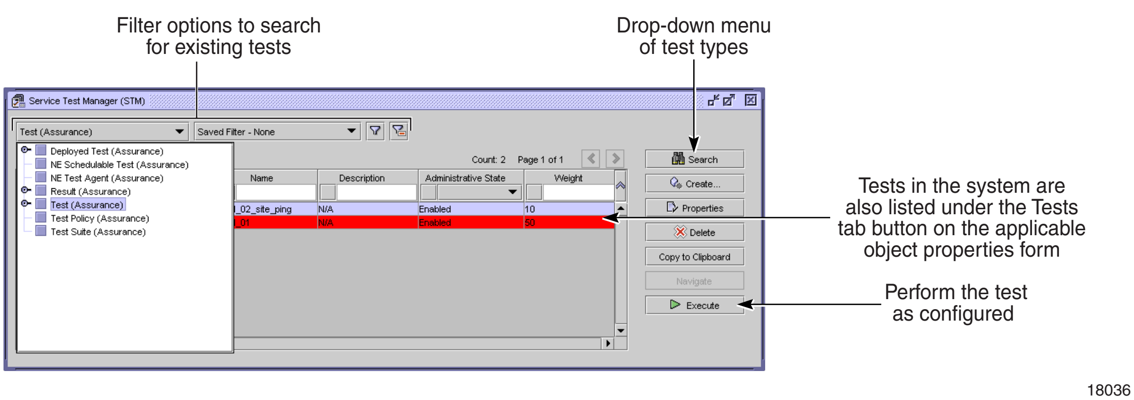
Service assurance test management and configuration

There are two main types of forms for the service assurance test manager.

- Browse and list manager, to generate lists of OAM diagnostics and to run OAM diagnostics
- Configuration form, to create or modify service assurance tests and review the results of service assurance tests

Figure 38-7 shows the browse and list manager form.

Figure 38-7 Service assurance test manager browse and list form



Each service assurance test configuration form contains multiple tabs. Figure 38-8 shows a sample service assurance OAM test with the General tab displayed.

Figure 38-8 Service assurance OAM test configuration form - General

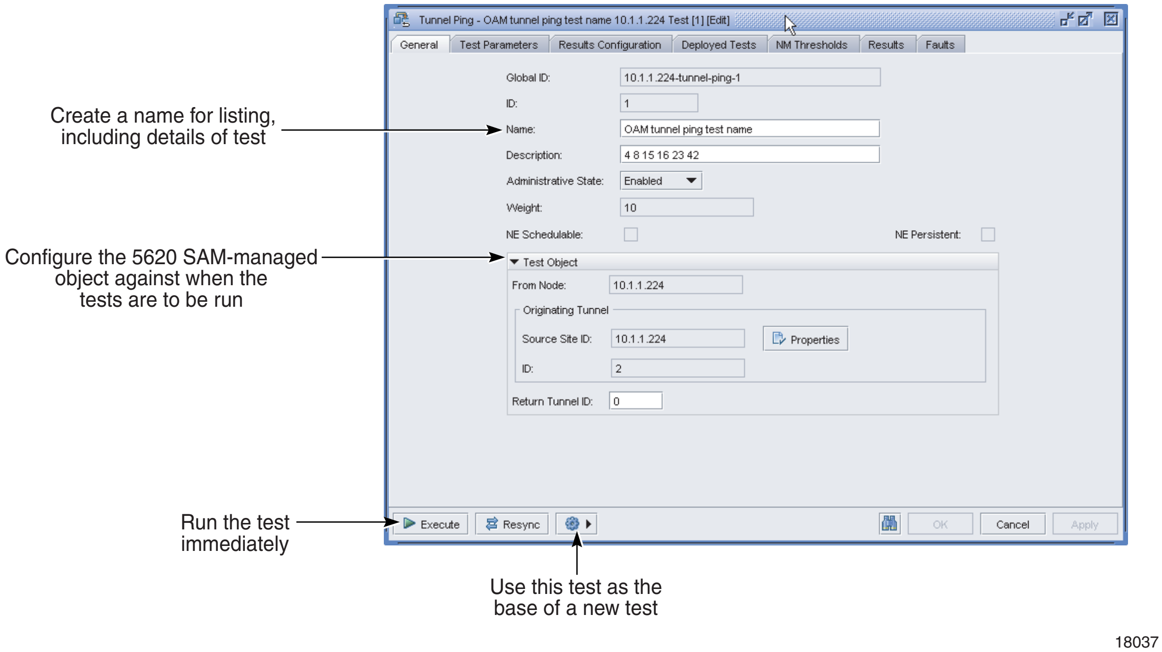


Figure 38-9 shows the same sample service assurance OAM test with the Test Parameters tab displayed.

Figure 38-9 Service assurance OAM test configuration form - Test Parameters tab

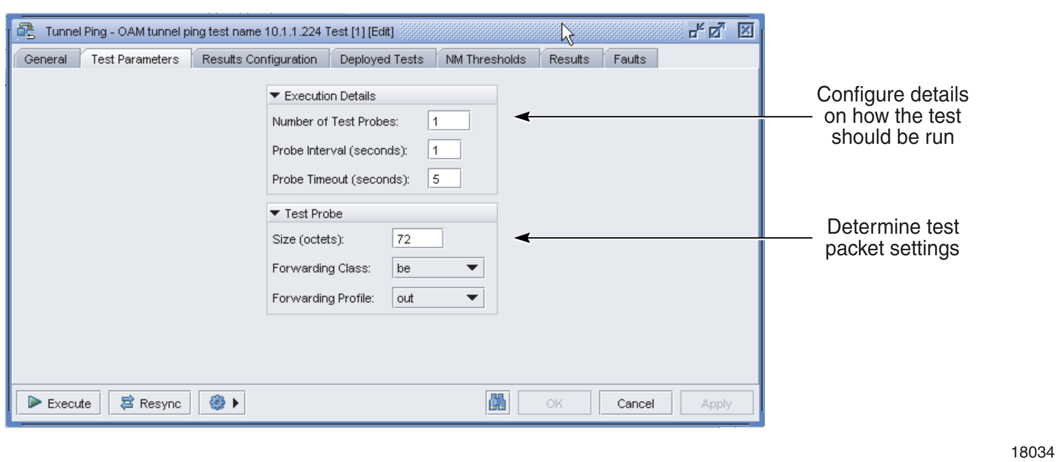


Figure 38-10 shows the same sample service assurance OAM test with the Results Configuration tab displayed.

Figure 38-10 Service assurance OAM test configuration form - Results Configuration

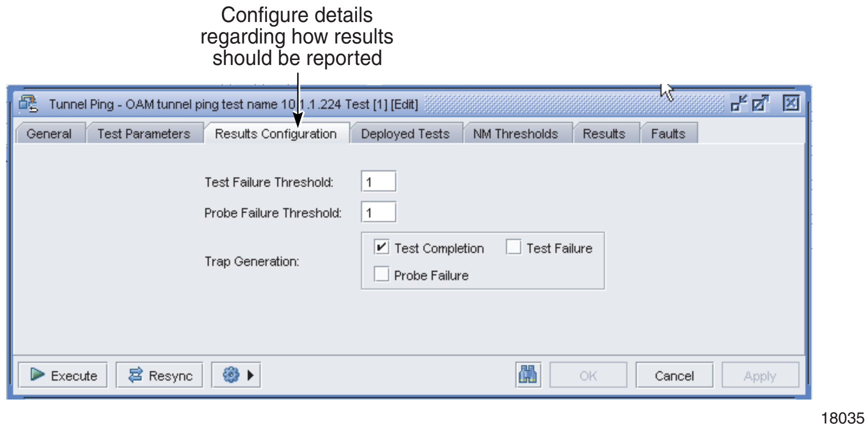


Figure 38-11 shows the same sample service assurance OAM test with the Results tab displayed. Selecting the Results tab button opens an additional form, which provides detailed test results, including OAM test packet details, when the OAM test involves sending test packets.

Figure 38-11 Service assurance OAM test configuration form - Results

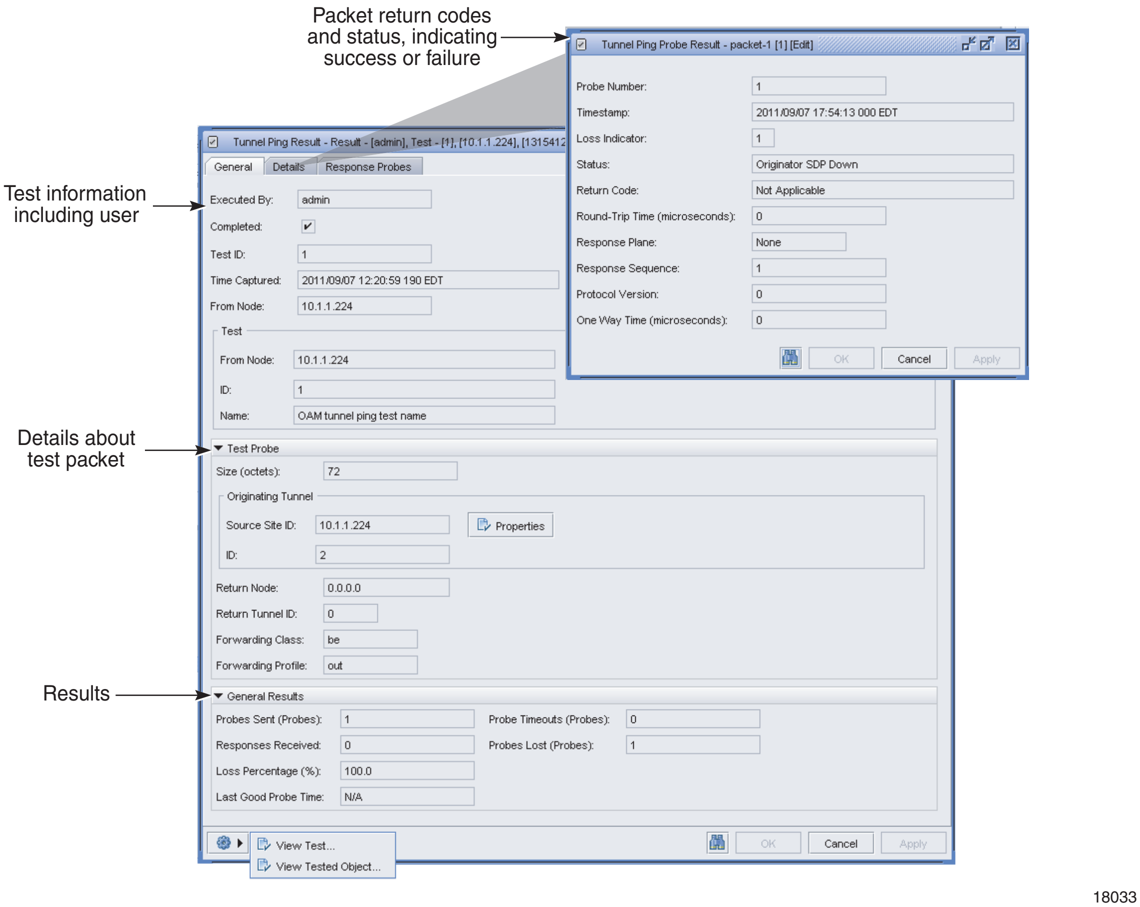
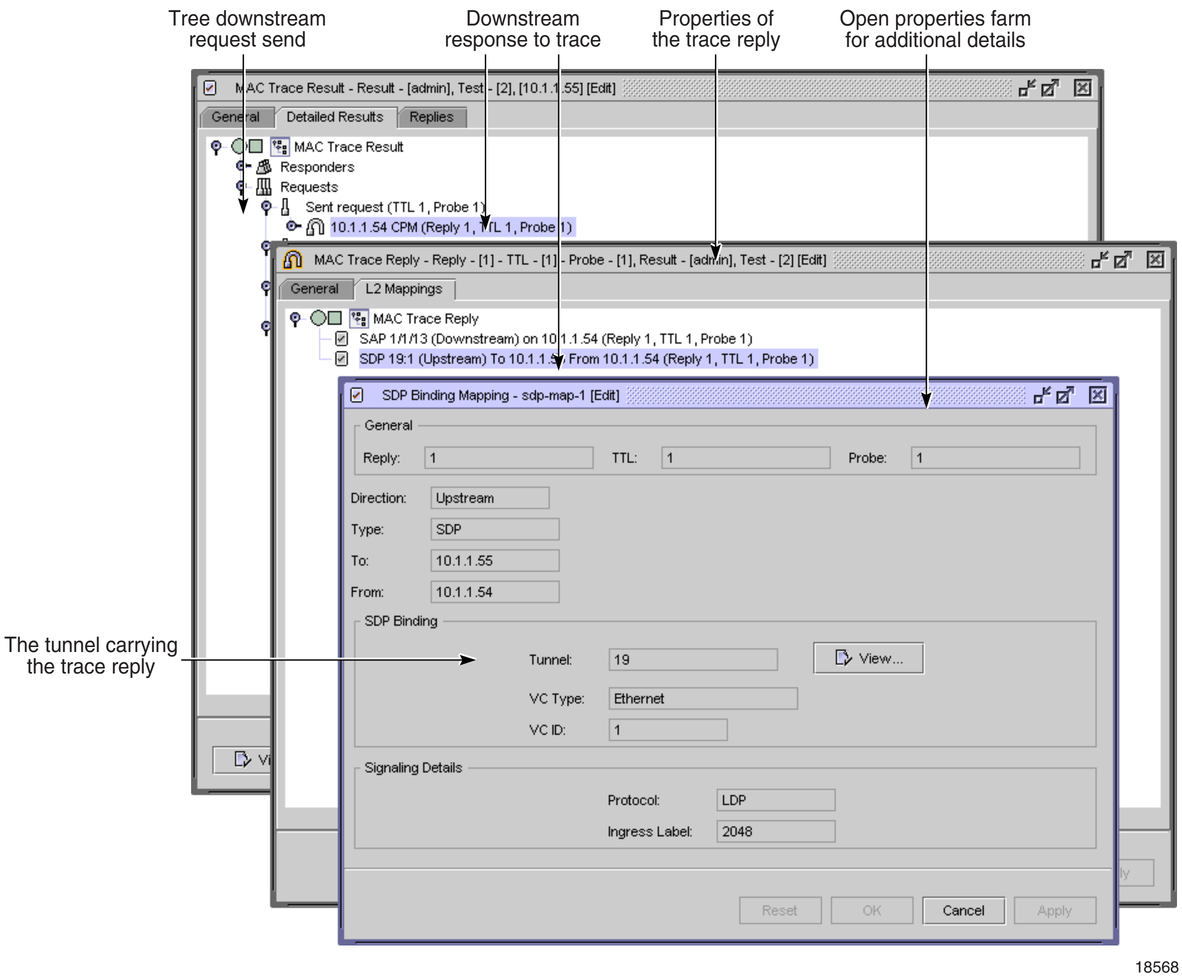


Figure 38-12 shows the information from a sample MAC trace. Trace probe information is available from the Detailed Results tab. Continue to navigate down from the trace requests to view result information.

Figure 38-12 Service assurance OAM test probe and trace results details



38.2 Sample OAM diagnostic test configuration

Figure 38-13 shows a sample OAM diagnostic sequence, illustrating how you can use multiple OAM tests to verify service creation and diagnose service problems. This sample shows a VPLS.

Figure 38-13 Sample OAM diagnostic sequence for a VPLS

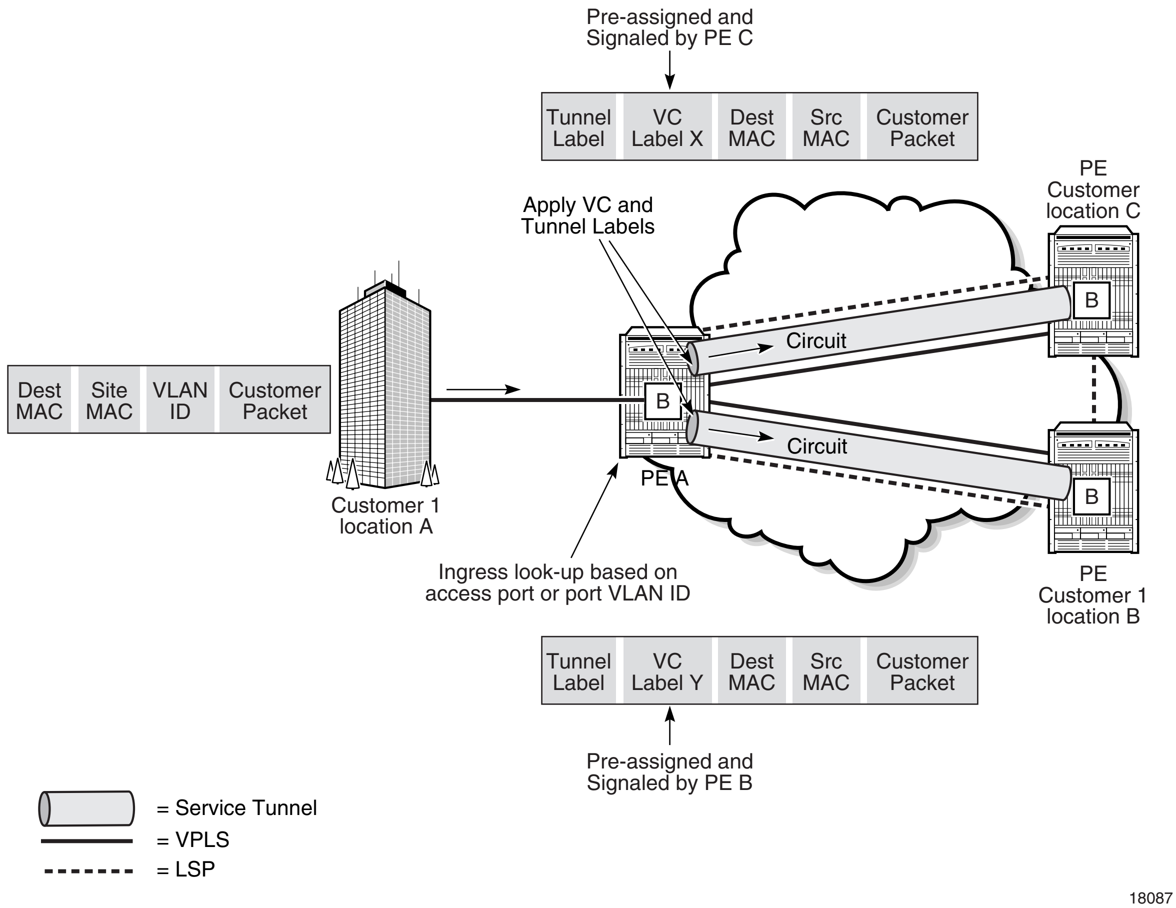


Table 38-2 lists the high-level tasks necessary to configure this sample.

Table 38-2 Sample OAM diagnostic configuration for a service

Task	Description
Service creation and OAM validation	
1. MPLS and LSP creation	Create an MPLS network and LSPs for use by the service tunnels connecting the VPLS sites. Test the validity of the LSPs using LDP tree trace or LSP ping. If the results indicate a problem with the path, use LSP trace to check the specific MPLS path for the device causing the ping failure.
2. Service tunnel creation	Create a service tunnel that uses the MPLS LSP created earlier and perform a tunnel ping on the service tunnel to verify tunnel connectivity. Create all tunnels necessary to interconnect the VPLS sites, and repeat the tunnel ping to ensure tunnel connectivity. After all of the tunnels are created, use the tunnel ping remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity.

(1 of 2)

Task	Description
3. Service creation	Create a service using the service tunnels to interconnect the VPLS sites, either using mesh or spoke service tunnel bindings. Use a service site ping between each VPLS site device and its neighboring sites to verify service configuration consistency.
4. MAC diagnostics	Connect the CPE devices to the VPLS and verify traffic. Use MAC trace from the edge devices to verify MAC address learning by the VPLS sites and to ensure that the correct associations are made between MAC addresses and the service tunnels or SAPs to which they are bound. Use MAC ping against an unknown MAC address to verify that no response is returned. Use MAC populate to create an OAM-specific MAC address. Use MAC ping and MAC trace against the created MAC address to verify that customer traffic is not affected by the additional MAC address. Use MAC purge to remove the created OAM MAC address.
Service OAM diagnostics	
1. Diagnose traffic flow problems at a specific MAC address	Use MAC ping against the MAC address to which traffic is not flowing. Use the source and destination MAC address to simulate customer traffic routes as closely as possible. Use MAC trace to pinpoint the location of the traffic failure. Check for MAC filter rules or MAC table sizes to identify possible causes of the failure, for example, incorrect configurations.
2. Diagnose the components of the service	Use service site ping to test the potential next hops to ensure consistent configuration. Use tunnel ping to the far end of the tunnel using the remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity. Use LSP ping to determine if the tunnel is working. Use an LSP trace to determine if an intervening device is down.

(2 of 2)

38.3 Workflow to use OAM diagnostic tests

1 Create the transport network and customer services.

2 Monitor customer services or troubleshoot the transport network before you commission, according to your company's policies.

3 When the creation of a tunnel needs to be tested, or a customer service is compromised, use the service assurance tools to troubleshoot the problem.

Note 1 — All of the tests mentioned in this workflow are used on an as-required basis.

Note 2 — Not all service assurance tools are applicable to every NE managed by the 5620 SAM.

i Use MTU ping to troubleshoot and resolve tunnel and service problems that are related to frame size across all equipment that is used by the service or tunnel. See Procedures 38-1 and 38-2 for more information.

ii Use tunnel ping to troubleshoot and resolve tunnel and service problems that are related to issues that circuits may have transmitting traffic across the GRE or MPLS network. See Procedures 38-3 and 38-4 for more information.

iii Perform Ethernet CFM tests to provide path discovery and fault detection, isolation, and notification in an L2 network. As required, perform any of the following tests:

- CFM Global MEG OAM; see Procedure 38-5.
- CFM CC OAM; see Procedure 38-6.
- CFM loopback; see Procedure 38-7.
- CFM link trace; see Procedure 38-8.
- CFM Eth test; see Procedure 38-9.
- CFM one-way delay; see Procedure 38-10.
- CFM two-way delay; see Procedure 38-11.
- CFM single-ended loss; see Procedure 38-12.
- CFM two-way SLM; see Procedure 38-13.

iv Use service site ping to troubleshoot and resolve service problems that are related to the end-to-end connectivity of a customer service within the provider network. See Procedure 38-22 for more information.

v Use VCCV ping and VCCV trace to troubleshoot and resolve issues that are related to VLL services. See Procedures 38-23 and 38-24 for more information.

vi Use LDP tree trace to detect and discover available routers for ECMP routing. See Procedure 38-29 for more information.

vii Use LSP ping and LSP trace to troubleshoot and resolve problems that are related to MPLS LSPs, LDPs, and MPLS paths. See Procedures 38-25 and 38-26 for more information.

viii Use P2MP LSP Ping and P2MP LSP Trace to perform in-band LSP connectivity tests. See Procedures 38-27 and 38-28 for more information.

ix Use MAC ping (Procedure 38-17), MEF MAC Ping (Procedure 38-18), MAC trace (Procedure 38-19), MAC populate (Procedure 38-15), MAC purge (Procedure 38-16), and CPE ping (Procedure 38-20) to troubleshoot and resolve problems that are related to FIBs and MAC addressing. The tests are used in combination; for example, MAC populate to inject a MAC address into the network, MAC ping to determine where the address was learned, MAC trace to determine the path, CPE ping to test the VPLS, and MAC purge to remove the injected MAC address.

x Use ANCP loopback to send OAM messages to the access node. See Procedure 38-21 for more information.

xi Use VPRN ping, VPRN trace, ICMP ping and ICMP trace to troubleshoot and resolve problems with a VPRN service. See Procedures 38-14, 38-35, and 38-36 for more information.

xii Use ATM ping and ATM loopback to test ATM PVC connections. See Procedures 38-33 and 38-34 for more information.

xiii Use multicast FIB ping to troubleshoot and resolve problems with the multicast component of a VPLS. See Procedure 38-32 for more information.

xiv Use multicast router information and multicast trace to troubleshoot and resolve problems with the multicast component of a VPRN service. See Procedures 38-30 and 38-31 for more information.

xv Use ICMP ping (Procedure 38-35), ICMP trace (Procedure 38-36), and DNS ping (Procedure 38-37) to troubleshoot and resolve problems with IP reachability.

xvi Use Procedure 38-42 to configure an 802.3ah EFM diagnostic at the NE or port level.

xvii (OmniSwitch only) Use OmniSwitch ping and traceroute scripts to troubleshoot and resolve problems with IP reachability on an OmniSwitch. See Procedures 38-38, 38-40, and 38-41 for more information.

xviii (OmniSwitch only) Use OmniSwitch advanced loopback to troubleshoot and resolve problems on an OmniSwitch port. See Procedure 38-39 for more information.

xix (OmniSwitch only) Use Procedure 38-43 to configure an 802.3ah EFM diagnostic on an OmniSwitch at the NE or port level.

4 Use Procedures 38-46 and 38-47 to configure NM threshold-crossing alarms for OAM tests that are NE-schedulable and non-NE-schedulable, respectively.

5 Use Procedure 38-50 to set STM managed device test limits.

6 Use the OAM tool diagnostic response messages and results form information to resolve the customer service problem. See Procedures 38-44 and 38-45 for more information.

7 Use Procedures 38-48 and 38-49 to edit or delete an OAM diagnostic test, respectively.

38.4 OSS OAM Test Results file retrieval

OSSI clients can use the <registerSasLogToFile> method to receive OAM logs that are based on specific class types. Clients must register to receive the logs, and if no client registers, no logs are created. Refer to the *5620 SAM XML OSS Interface Developer Guide* for detailed information on OSSI client operations.

OAM data is exported to the file after the data is read from the NE. The file is saved to a specified directory on the 5620 SAM server.

Prior to enabling OSSI clients to receive Test Results files, you should configure the Default Test Result Storage, Log Retention Time (minutes), and Log Rollover Time (minutes) parameters as required. These are accessed by clicking Administration→System Preferences and then clicking the Test Manager tab.

Note — The 5620 SAM server verifies the connectivity of the 5620 SAM-O client that is specified in the registerSasLogtoFile method using the jmsClientId input parameter. The server deregisters the LogToFile request and the 5620 SAM-O client if the JMS session is disconnected.

Alcatel-Lucent recommends that you run the registerSasLogToFile method every time the 5620 SAM-O client establishes a JMS session.

Table 38-3 describes the input parameters of the <registerSasLogToFile> method.

Table 38-3 <registerSasLogToFile> method input parameters

Input parameter	Description	Values
fullClassName	Package qualified class name in dot separated format.	A comma-separated list of OAM results
compress	Specifies if export files should be compressed when created. A value of true saves files with gzip compression and a filename extension of gz. The default is false. This parameter is optional.	—
continueOnFailure	Specifies whether or not to continue processing requests in this stream if an exception occurs. A value of true continues processing the requests. The default is false. This parameter is optional.	OSSI requests can be sent with this option set to true.
dirName	The relative path to the subdirectory where the log files are to be saved. The path is relative to the OSS XML export directory /opt/5620sam/server/xml_output	—
jmsClientId	The JMS client ID that is notified when a new export file is created for the specified parameters. A notification message is sent to each client that registers for OAM logs every time an export file is created that is related to that client.	See the *5620 SAM XML OSS Interface Developer Guide* for more information about JMS client ID formats.
resultFilter	(Optional) Specifies the attributes that are to be included in the exported OAM log. You can use the resultFilter parameter to reduce the size of the export file.	<attribute>*attribute_name*</attribute>

The OAM log files are created on the 5620 SAM main server. Export file names are unique and are created under the directory that you specify in the registration request. For example:

/opt/5620sam/server/xml_output/oam/<dir_name>

OAM log retrieval example using the <registerSasLogToFile> method

Code 38-1 shows a sample request for an OAM log file using the <registerSasLogToFile> method.

Code 38-1: Sample request to export OAM logs to an XML file using a filter

```
<registerSasLogToFile xmlns="xmlapi_1.0">
         <fullClassName>
          sas.TestResult,
          sas.TraceHop
         </fullClassName>
         <dirName>jmsclientdir</dirName>
         <jmsClientId>oam@1001</jmsClientId>
    <resultFilter>
       <attribute>testSuiteId</attribute>
       <attribute>testId</attribute>
       <attribute>fromNodeId</attribute>
       <attribute>neTestRunIndex</attribute>
       <attribute>resultStatus</attribute>
    </resultFilter>
</registerSasLogToFile>
```

38.5 OAM diagnostic tests procedures

Use the following procedures to create and execute OAM diagnostic tests.

Procedure 38-1 To create and run an MTU ping OAM diagnostic from a service tunnel

Use the MTU ping diagnostic to find the largest valid frame size.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels appears.

3 Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.

4 Click on the Tests tab button.

5 Click on the MTU Ping tab button.

6 Click on the Create button. The MTU Ping (Create) form opens with the General tab displayed. The form displays information about the service tunnel being tested and the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

8 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)

Note — If the step size is small but the end message size is large, the amount of time to complete the MTU ping may be many minutes. Ensure that you have an appropriate step size that reflects the range of MTU packet sizes you want to test.

9 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Perform the MTU ping.

i Click on the Execute button in the MTU Ping (Edit) form. The MTU ping diagnostic starts. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab button. The list of MTU ping OAM probes sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- frame size sent
- OAM diagnostic status
- diagnostic code returned

See Procedure 38-45 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results. For example, the status message Response Received indicates that the MTU OAM diagnostic completed successfully.

v Close the form.

12 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 38-2 To create an MTU ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create MTU Ping from the Create contextual menu. The MTU Ping (Create) form opens.

4 Configure the parameters described in Procedure 38-1. You must additionally configure the source of the service tunnel.

i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

ii Click on the Search button.

iii Select a tunnel from the list.

iv Click on the OK button. The MTU Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

7 Click on the Execute button to start the ping. A deployed test is created and run.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-3 To create and run a tunnel ping OAM diagnostic from a service tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels opens.

3 Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.

4 Click on the Tests tab button.

5 Click on the Tunnel Ping tab button.

6 Click on the Create button. The Tunnel Ping (Create) form opens with the General tab displayed. The form displays information about the circuit being tested, including the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Return Tunnel

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

8 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile

The Probe Interval (seconds) parameter has an effect only when multiple probes are to be sent.

Ensure that you configure the Forwarding Class parameter to work with the services that use the tunnel.

9 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Confirm the action. The created tunnel ping test appears in the list of tests on the Tunnel Ping tab of the Tunnel (Edit) form.

12 Perform the tunnel ping OAM diagnostic:

i Click on the Execute button in the Tunnel Ping (Edit) form. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab button. The list of tunnel ping OAM packets sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- OAM diagnostic status
- diagnostic code returned

See Procedure 38-45 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results.

v Close the form.

13 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 38-4 To create a tunnel ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create SDP Ping from the Create contextual menu. The Tunnel Ping (Create) form opens.

4 Configure the parameters described in Procedure 38-3. You must additionally configure the source of the service tunnel.

i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

ii Configure the filter criteria.

iii Click on the Search button.

iv Select a tunnel from the list.

v Click on the OK button. The Tunnel Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Click on the Execute button to start the tunnel ping. A deployed test is created and run.

7 Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-5 To create and execute a CFM Global MEG OAM diagnostic

Perform this procedure to manually create and execute a CFM Global MEG test.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button and choose Ethernet CFM→CFM Global MEG from the menu. The Global Maintenance Entity Group, Test (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

4 To configure parameters in the Maintenance Domain tab, Maintenance Entity Group and Initial MEG configuration, see Procedure 80-1 for more information.

5 Click on the Apply button. The form displays additional buttons and tabs.

6 To execute the test, click on the Test tab and select the Test to be executed. Select the test and click on the Properties button, the CFM Continuity Check (Edit) form.

7 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

8 Close the CFM Continuity Check Test (Edit) form.

Procedure 38-6 To create and execute a CFM CC OAM diagnostic

Perform this procedure to manually create and execute a CFM CC test.

Note — The 5620 SAM automatically creates a CFM CC test when you create an MD and global MEG. You can execute an automatically created test using the STM, or from the Tests tab of a MEG.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button and choose Ethernet CFM→CFM Continuity Check from the menu. The CFM Continuity Check Test (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- Duration (minutes)

4 If you are configuring the test for a 7705 SAR, configure the parameters in the Initial Dual Ended Loss Test Options panel:

- Enable Test
- Alarm Threshold (%)
- Alarm Clearing Threshold (%)

5 Click on the Select button. The Select Maintenance Entity Group form opens.

6 Specify a search filter, if required, and click on the Search button. A list of MEGs is displayed.

7 Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG is displayed on the CFM Continuity Check Test (Create) form.

8 Click on the Apply button. The form displays additional buttons and tabs.

9 To execute the test, click on the Execute button on the CFM Continuity Check (Edit) form.

10 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

11 Close the CFM Continuity Check Test (Create) form.

Procedure 38-7 To create and execute a CFM loopback diagnostic

Perform this procedure to manually create and execute a CFM loopback test. You can create multiple CFM loopback tests for an originating MEP.

Note — The maximum number of continuous CFM loopback tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Loopback from the contextual menu. The CFM Loopback Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable

Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Loopback form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Loopback form closes, and the CFM Loopback (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Loopback form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Loopback form closes, and the CFM Loopback (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to select the destination MIP. The Select MIP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

Note — MIP selection is not supported for OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, go to step 13.

13 Configure the MEP Transmit LBM Information parameters:

- Data Size
- VLAN Priority
- Number of Loopback Sent
- VLAN Drop Enable

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)
- Continuous Execution

16 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-8 To create and execute a CFM link trace diagnostic

Note — The maximum number of continuous CFM link trace tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

However, it is recommended that number of continuous CFM link trace tests executed should be kept well below the maximum allowed limit.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Link Trace from the Create contextual menu. The CFM Link Trace (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable

Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Link Trace form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Link Trace form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, go to step 13.

13 Configure the MEP Transmit LTM Information TTL parameter.

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- TTL
- Continuous Execution

16 Click on the Results Configuration tab and configure the parameters:

- Maximum Failures
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-9 To create and execute a CFM Eth test diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Eth Test from the Create contextual menu. The CFM Eth Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Eth Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Eth Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the MEP information.

11 Perform one of the following.

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

12 Configure the MEP Transmit LBM Information parameters:

- Data Size (octets)
- VLAN Priority

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-10 To create and execute a CFM one-way delay diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM One Way Delay Test from the Create contextual menu. The CFM One Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM One Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM One Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM One Way Delay Test form closes, and the CFM One Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

- **a** Select a MEP as the test destination. Perform the following steps.
  - **i** Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM One Way Delay form opens.
  - **ii** Select an entry and click on the OK button. The Select MEP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.
- **b** Select a MIP as the test destination. Perform the following steps.
  - **i** Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM One Way Delay form opens.
  - **ii** Select an entry and click on the OK button. The Select MIP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.
- **c** Select an unmanaged MEP as the test destination. Perform the following steps.
  - **i** Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM One Way Delay form opens.
  - **ii** Select an entry and click on the OK button. The Select Unmanaged MEP - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form refreshes.

12 Configure the Priority parameter in the MEP Transmit LBM Information panel.

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-11 To create and execute a CFM two-way delay diagnostic

Note — The maximum number of continuous CFM two-way delay tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Two Way Delay Test from the Create contextual menu. The CFM Two Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable

Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Two Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Two Way Delay form closes, and the CFM Two Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Two Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

Note — MIP selection is not supported on OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, go to step 13.

13 Configure the MEP Transmit DMM Information VLAN Priority parameter.

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Continuous Execution

16 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-12 To create and execute a CFM single-ended loss diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Single Ended Loss Test from the Create contextual menu. The CFM Single Ended Loss Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Single Ended Loss Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Single Ended Loss Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the MEP information.

11 Choose a destination MEP:

  i Click on the Select MEP button beside the Target MAC Address parameter. The Select MEP - CFM Single Ended Loss Test form opens.

  ii Double-click on an entry in the list, or choose an entry and click on the OK button. The Select MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form refreshes.

12 Configure the following parameters in the MEP Transmit LMM Information panel:

- Priority
- Count
- Interval

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-13 To create and execute a CFM two-way SLM (Synthetic Loss Measurement) diagnostic

Note — The maximum number of continuous CFM two-way SLM tests that can be executed is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Two Way SLM from the Create contextual menu. The CFM Two Way SLM Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NM Administrative State
- NE Schedulable

Note — If the NE Schedulable parameter is enabled, two additional tabs are displayed for the form, Test Parameters and Results Configuration.

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Two Way SLM Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Two Way SLM Test form closes, and the CFM Two Way SLM Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Two Way SLM Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Two Way SLM Test form closes, and the CFM Two Way SLM Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

Note — MIP selection is not supported on OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - Two Way SLM form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM (Create) form refreshes.

12 If the NE Schedulable parameter was enabled in step 4 then go to step 15. Otherwise, go to step 13.

13 In the MEP Transmit SLM Information panel, configure the following parameters:

- Priority
- Interval (seconds)
- Timeout (seconds)
- Data Size (octets)
- Send Count (packets)

14 Go to step 17.

15 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)
- Continuous Execution

16 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation
- Accounting Files
- Test Result Storage

The Trap Generation parameter is only configurable when the Accounting Files parameter is disabled.

The Test Result Storage parameter is only configurable when the Accounting Files parameter is enabled.

17 Click on the Apply button to save the changes.

18 To execute the test, click on the Execute button.

19 Click on the Results tab button to view the test results. See Procedure 38-44 for information about test results.

Procedure 38-14 To configure and run VPRN OAM diagnostics from a service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Service Manager form opens.

2 Filter to list only the services on which you want to perform OAM diagnostics and click on the Search button.

3 Choose a service from the list and click on the Properties button. The Service (Edit) form opens.

4 Click on the Sites tab button.

5 Choose a site or sites from the list and click on the Properties button. The Site (Edit) form opens.

6 Click on the Tests tab button.

7 Configure and run a VPRN ping or VPRN trace OAM diagnostic.

a To configure and run a VPRN ping:

i Click on the VPRN Ping tab. A list of VPRN diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Ping form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Ping form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Source IP Address
- Target IP Address
- Time To Live
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

viii Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run a VPRN trace:

i Click on the VPRN Trace tab. A list of VPRN trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN Trace (Create) form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Trace form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Trace form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Source IP Address
- Target IP Address
- Initial Time to Live
- Maximum Time to Live
- DiffServ Field
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

viii Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Choose the diagnostic from the list.

xii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 Configure and run an ICMP ping or ICMP trace OAM diagnostic.

a To configure and run ICMP ping:

i Click on the ICMP Ping tab. A list of ICMP diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- From IP Address
- Target IP Address
- Next Hop Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment

v Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

vi Click on the Apply button to save the changes.

vii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run ICMP trace:

i Click on the ICMP Trace tab. A list of ICMP trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Trace form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- From IP Address
- Target IP Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Maximum Time to Live
- DiffServ Field
- Time To Wait (milliseconds)

v Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

vi Click on the Apply button to save the changes.

vii Choose the diagnostic from the list.

viii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

Procedure 38-15 To configure and run MAC populate OAM diagnostics

You can also perform the diagnostic from the Tests tab of a VPLS or Epipe VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Populate from the Create contextual menu. The MAC Populate (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send Via Control Plane
- Flood
- Force OAM
- Age (seconds)
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Execute button to start the MAC populate diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-16 To configure and run MAC purge OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Purge from the Create contextual menu. The MAC Purge (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send Via Control Plane
- Inhibit Learning
- Flood
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Properties button.

9 Click on the Execute button to start the MAC purge diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-17 To configure and run MAC ping OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→ MAC Ping from the Create contextual menu. The MAC Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Target MAC Address
- Source MAC Address
- Service Name
- Name

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Properties button.

10 Click on the Execute button to start the MAC ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-18 To configure and run MEF MAC ping OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS.

Note — MEF MAC Ping must run simultaneously in both directions between the source and destination VPLS sites. Configure a test from the source VPLS site to the destination VPLS site and from the destination VPLS site to the source VPLS site.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MEF MAC Ping from the Create contextual menu. The MEF MAC Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Target MAC Address

5 Choose a VPLS service.

  i Click on the Select button in the Service panel. The Select Service - MEF MAC Ping form opens.

  ii Configure the filter criteria and click on the Search button. A list of VPLSs appears.

  iii Choose a VPLS and click on the OK button. The Select Service - MEF MAC Ping form closes.

6 When you choose a VPLS, the Site panel appears on the form. Choose a VPLS site that belongs to the selected VPLS.

  i Click on the Site panel Select button. The Select Site - MEF MAC Ping form opens.

  ii Configure the filter criteria and click on the Search button. A list of VPLS sites appears.

  iii Choose a VPLS site and click on the OK button. The Select Site - MEF MAC Ping form closes.

7 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)

8 Click on the Results Configuration tab button and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

9 Click on the OK button to save the changes.

10 Choose the created test from the list of OAM diagnostics.

11 Click on the Execute button to start the MEF MAC ping. A deployed test is created and run. Click on the Deployed Tests tab button to open the deployed test and view the current state of the test. When the test is complete, the deployed test is removed and you can view the results.

12 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- round trip jitter
- round trip latency
- round trip frame loss

Procedure 38-19 To configure and run MAC trace OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Trace from the Create contextual menu. The MAC Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Target MAC Address
- Source MAC Address
- Initial Time to Live
- Maximum Time to Live
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Profile
- Forwarding Class

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the MAC trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-20 To configure and run CPE ping OAM diagnostics

You can also perform this diagnostic from the Test tab of a VPLS.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create CPE Ping from the Create contextual menu. The CPE Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Service Name
- Name
- Destination Path Address
- Source IP Address
- Source MAC Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- VC's Label Time Live
- Send Via Control Plane
- Reply Via Control Plane
- Forwarding Profile
- Forwarding Class

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Click on the Search button to display the list of OAM diagnostics.

9 Double-click on the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the CPE ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab.

12 To display the test results, select the test from the CPE Ping Result list and click on the Properties button. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-21 To configure and run ANCP loopback diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create ANCP Loopback from the Create contextual menu. The ANCP Loopback (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

5 Click on the Select button beside the System ID (Loopback Ip Address) parameter. The Select Originating Node - ANCP Loopback form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The Select Originating Node - ANCP Loopback form closes, and the ANCP Loopback (Create) form refreshes.

9 Click on the Test Parameters tab button and perform one of the following steps.

  a Configure the ANCP loopback diagnostic for a subscriber ID.

    i Set the Target Type parameter to Subscriber Ident String.

    ii Configure the Subscriber Ident String parameter.

  b Configure the ANCP loopback diagnostic for an ANCP string.

    i Set the Target Type parameter to ANCP String.

    ii Configure the ANCP String parameter.

10 Configure the parameters:

- Count
- Timeout (seconds)

11 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

12 Click on the Apply button to save changes.

13 Click on the Execute button to start the ANCP loopback diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete you can view the results.

14 Click on the Results tab to view the test results.

15 Select the test from the ANCP Loopback Result list and click on the Properties button. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-22 To configure and run service site ping OAM diagnostics

1. Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2. Click on the Create button.

3. Choose Service→ Service Site Ping from the Create contextual menu. The Service Site Ping (Create) form opens with the General tab displayed.

4. Configure the parameters:

   - ID
   - Auto-Assign ID
   - Name
   - Description
   - Administrative State
   - System ID (Loopback Ip Address)

5. Click on the Test Parameters tab button and configure the parameters:

   - Target IP Address
   - Service ID
   - Use Local Tunnel
   - Use Remote Tunnel

   When you set the target IP address, then choose a service ID, only service IDs from the selected site are available. When you set the Use Local Tunnel and Use Remote Tunnel parameters, the test becomes a ping that tests the service tunnel bindings between the service sites.

6. Click on the Results Configuration tab button and configure the parameters:

   - Probe History Size (rows)
   - Test Failure Threshold
   - Probe Failure Threshold
   - Trap Generation

7. Click on the OK button to save the changes.

8. Choose the created test from the list of OAM diagnostics and click on the Properties button.

9. Click on the Execute button to start the service site ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10. View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

    - Number of Probes Sent
    - Time Last Response
    - Number of Responses Received

Procedure 38-23 To configure and run VCCV ping OAM diagnostics

You can also perform a VCCV ping from a VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Ping from the Create contextual menu. The VCCV Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Select button in the First Spoke SDP Binding panel. The Select First Spoke SDP Binding - VCCV ping form appears.

6 Click on the Search button.

7 Select the first spoke SDP binding and click on the OK button. The Select First Spoke SDP Binding - VCCV ping form closes.

8 Click on the Select button in the Downstream SDP Binding panel. The Select downstream spoke SDP Binding - VCCV ping form appears.

9 Click on the Search button.

10 Select the downstream spoke SDP binding and click on the OK button. The Select downstream spoke SDP Binding - VCCV ping form closes.

11 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type parameter

12 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

13 Click on the OK button to save the changes.

14 Choose the created test from the list of OAM diagnostics.

15 Click on the Execute button to start the VCCV ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

16 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- IP address of the destination and far-end device
- Time Last Response
- Number of Responses Received
- Response Time
- Loss indicator, a value of 0 indicates that the test packet was received and a value of 1 indicates that the test packet was lost

Procedure 38-24 To configure and run VCCV Trace OAM diagnostics

You can also perform a VCCV Trace test from a VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Trace from the Create contextual menu. The VCCV Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Select button in the First Spoke SDP Binding panel. The Select First Spoke SDP Binding - VCCV Trace form appears.

6 Click on the Search button.

7 Select the first spoke SDP binding and click on the OK button. The Select First Spoke SDP Binding - VCCV Trace form closes. The parameters in the First Spoke SDP Binding block are populated.

8 Configure the parameters:

- Initial Time to Live
- Maximum Time to Live

9 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type parameter

10 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

11 Click on the OK button to save the changes. The VCCV Trace (Create) form closes.

12 Click on the Test (Assurance) item in the Service Test Manager form and then click the Search button.

13 Choose the created test from the list of tests in the Test (Assurance) block.

14 Click on the Execute button to start the VCCV Trace test. A deployed test is created and run.

15 Click on the Properties button. The VCCV Trace (Edit) form opens with the General tab displayed.

16 Click on the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

17 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from nodes in path

Procedure 38-25 To configure and run LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Site ID
- IP Address
- LDP Prefix
- LDP Prefix Length
- Destination Path Address
- Next Hop Interface Name
- Next Hop Interface Address
- Return LSP

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Double-click on the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the LSP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-26 To configure and run LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Site ID
- IP Address
- LDP Prefix
- LDP Prefix Length
- Destination Path Address
- Probe Failure Threshold
- Next Hop Interface Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 38-27 To configure and run P2MP LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Ping from the Create contextual menu. The P2MP LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click the Select button in the P2MP Dynamic Lsp panel to choose the P2MP Dynamic LSP you want to test.

6 Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test.

7 Configure the Select All S2L Paths parameter.

If you enabled the parameter, go to step 10.

8 Click on the S2L Paths tab.

9 Select the S2L paths that you want to test. A maximum of five can be selected.

10 Click on the Test Parameters tab and configure the parameters:

- Probe Timeout (seconds)
- Probe Interval (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

11 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

12 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 38-47 for details.

13 Click on the OK button to save the changes. The Service Test Manager form opens.

14 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Ping (Edit) form opens, with the General tab displayed.

15 Click on the Execute button to start the P2MP LSP ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

Note — When this test is performed on an existing Point-to-Multipoint LSP, up to five S2L paths can be selected. If none are selected, all available paths up to the limit of five will be pinged.

16 Click on the Results tab in the P2MP LSP Ping (Edit) form.

If you enabled the Select All S2L Paths parameter in step 7, the Results tab will show an entry for each path tested.

17 Select the test from the list and click on Properties. The P2MP LSP Ping Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed, its status, and the following test information:

- Number of Probes Sent
- Probe Timeouts
- Number of Responses Received
- Probes Lost

Note — The test results depend on the type of test you run. Refer to Procedure 38-44 for more information.

18 Click on the Details tab.

19 View the test results for the:

- Round Trip Time
- Outbound One Way Time
- Inbound One Way Time

20 Click on the Response Probes tab.

21 Select a response probe from the list and click on Properties. The P2MP LSP Ping Probe Result form opens.

Note — The test results depend on the type of test you run. Refer to Procedure 38-44 for more information.

22 View details on the response probe, including:

- Status
- Round-Trip Time
- Response sequence

23 Repeat steps 17 to 22 for all tested S2L paths.

Note — Refer to the Service assurance test management and configuration in Section 38.1 and to Chapter 78 for more information on viewing test results.

Procedure 38-28 To configure and run P2MP LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Trace from the Create contextual menu. The P2MP LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

5 Click the Select button in the P2MP Dynamic Lsp panel to choose the P2MP Dynamic LSP you want to test.

6 Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test.

7 Click the Select button in the S2L Destination Address panel to choose the S2L Destination Address you want to test.

8 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

9 Click on the Results Configuration tab and configure the parameters:

- Maximum Failures
- Trap Generation

10 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 38-47 for details.

11 Click on the OK button to save the changes. The Service Test Manager form opens.

12 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Trace (Edit) form opens, with the General tab displayed.

13 Click on the Execute button to start the P2MP LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

14 Click on the Results tab.

15 Select the test from the list and click on Properties. The P2MP LSP Trace Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed and its status.

Note — The test results depend on the type of test you run. Refer to Procedure 38-44 for more information.

16 Click on the Hops and Probes tab.

A tree view of the Hops and Probes associated with this test is provided.

17 Right-click on a Hop from the tree view and click on Properties.

The P2MP LSP Trace Hop (Edit) form is displayed, showing the General tab.

18 View the test results for the:

- Response Probe
- Round Trip Details
- Outbound One Way Trip Details
- Inbound One Way Trip Details

19 Right-click on a Probe from the tree view and click on Properties.

The P2MP LSP Trace Probe (Edit) form is displayed, showing the General tab.

20 View details on the probe, including:

- Response Probe
- LSP Details

21 Repeat this test for all required S2L paths. The test only evaluates one S2L path per execution.

Note — Refer to the Service assurance test management and configuration in Section 38.1 and to Chapter 78 for more information on viewing test results.

Procedure 38-29 To configure and run LDP Tree Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button. The test options are displayed in a drop-down menu.

3 Choose MPLS→Create LDP Tree Trace from the Create contextual menu. The LDP Tree Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Site ID
- LDP Prefix
- LDP Prefix Length

5 Click on the Test Parameters tab button and configure the parameters:

- Maximum Time to Live
- Timeout (seconds)
- Retry Counter
- Forwarding Class
- Profile
- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the LDP tree trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 Click on the Results tab. A list of LDP tree trace tests appears.

11 Choose a LDP tree trace from the list and click on the Properties button.

12 View the test results. The results depend on the type of test. See Procedure 38-44.

Procedure 38-30 To configure and run multicast router information OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mrinfo from the Create contextual menu. The mrinfo (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Site ID

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the Select button to choose a PIM interface. The Select PIM Interface form opens.

7 Select a PIM interface in the list and click on the OK button. The Select PIM Interface form closes, and the interface information is displayed on the mrinfo (Create) form.

8 Click on the OK button to save the changes.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the diagnostic request for multicast router information. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44.

Procedure 38-31 To configure and run multicast trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mtrace from the Create contextual menu. The mtrace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Site ID
- Source Address
- Destination Address
- Response Address

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Initial Time to Live
- Maximum Number of Hops

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44.

Procedure 38-32 To configure and run multicast FIB ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mfib Ping from the Create contextual menu. The MFIB Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Service Name
- Multicast Source
- Multicast Group
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Timeout (seconds)
- Reply Via Control Plane

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast FIB ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44.

Procedure 38-33 To configure and run an ATM OAM ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L1/L2→Create ATM Ping from the Create contextual menu. The ATM Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- ATM Interface ID

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Loopback Location (hex)
- Destination Type

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings. A confirmation window opens.

8 Click on the Yes button.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the ATM ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

12 To configure another ATM OAM ping, click on the Clear button and repeat steps 5 to 11. Otherwise, go to step 13.

13 Click on the Cancel button to close the form.

Procedure 38-34 To configure an ATM OAM loopback

ATM OAM loopback settings are configured globally on supported devices. However, a loopback must be enabled on an IES or VPRN SAP.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an ATM OAM loopback and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the ATM tab button.

4 Configure the parameters:

- ATM OAM Loopback Location ID
- ATM OAM Loopback Period
- Number of Tries for Up State
- Number of Tries for Down State

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 38-35 To configure and run an ICMP ping

You can also perform an ICMP ping from the Test tab of a VPRN or EIS service configuration form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→ ICMP Ping from the Create contextual menu. The ICMP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- Target IP Address
- Next Hop Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

Note — The NE Persistent test is not supported on OmniSwitch NEs.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter

10 To configure another ICMP ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 38-36 To configure and run an ICMP trace

You can also perform an ICMP trace from the Test tab of a VPRN or EIS.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create ICMP Trace from the Create contextual menu. The ICMP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- Target IP Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Maximum Time to Live
- DiffServ Field
- Time To Wait (milliseconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Current Hop Count
- Current Probe Count
- Minimum Round-Trip Time
- Round-Trip Jitter

Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

10 To configure another ICMP trace, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 38-37 To configure and run a DNS ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create DNS Ping from the Create contextual menu. The DNS Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback Ip Address)
- From IP Address
- Source IP Address
- DNS Server Type
- DNS Name
- DNS Server Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the DNS ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 38-44. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter
- Sum of Squares Round-Trip Time

10 To configure another DNS ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 38-38 To create an OmniSwitch OAM CLI script

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

Perform this procedure to create an OmniSwitch OAM CLI script using the sample scripts in Code 38-2 and Code 38-3.

1 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager form opens.

2 Choose CLI Script (Scripting) from the object drop-down list and click on the Create button. The CLI Script (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Type
- Use Latest Version
- Starting Point
- Continue On Command Failure
- Content Type

Enable the Use Latest Version parameter to associate all of the targets of the script with the latest version of the CLI script.

You must set the Content Type parameter to Velocity.

4 Perform the following steps to specify the script target types.

i Click on the Add button in the NE Types panel. The Select Property - CLI Script form opens.

ii Select one or more OmniSwitch NE types in the list and click on the OK button. The Select Property - CLI Script form closes, and the NE types are listed on the CLI Script (Create) form.

5 Click on the Apply button to apply the configuration.

6 Click on the Versions tab button.

7 Create the script by clicking on the Create button. The Script Editor *script_name* form opens.

8 Create the CLI script text by performing one of the following steps.

a Import an existing text file with a CLI script. You can create a text file by copying and pasting the text from the sample OmniSwitch ping shown in Code 38-2 or the sample traceroute script shown in Code 38-3 into a text editor.

i Choose File→Import from the Editor menu. The Import dialog box appears.

ii Choose the file to be imported and click on the Import button. The script appears in the script manager editor workspace.

iii Modify the script as required.

b Enter or copy and paste the CLI script text from the sample OmniSwitch ping shown in Code 38-2 or the sample traceroute script shown in Code 38-3 into the script manager editor workspace. .

The following ping and traceroute scripts are sample CLI scripts that can be used to run ping and traceroute tests. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating, configuring, and using scripts.

Code 38-2: Sample OmniSwitch OAM ping script

```
<velocityProperties>
```

```
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the system to ping (IPv4
xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>count</name>
        <uiName>Count:</uiName>
        <tooltip>Number of frames to be transmitted</tooltip>
        <type>Integer</type>
        <default>6</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>packed_size</name>
        <uiName>Packet Size:</uiName>
        <tooltip>Size of the data portion of the packet sent for this
ping, in bytes</tooltip>
        <type>Integer</type>
        <default>64</default>
        <required>true</required>
        <uiOrder>3</uiOrder>
        <min>1</min>
        <max>60000</max>
      </property>
      <property>
        <name>interval</name>
        <uiName>Interval (seconds):</uiName>
        <tooltip>Polling interval</tooltip>
        <type>Integer</type>
        <uiOrder>4</uiOrder>
        <default>1</default>
        <min>1</min>
        <max>10000</max>
      </property>
      <property>
        <name>timeout</name>
        <uiName>Timeout (seconds):</uiName>
        <tooltip>Number of seconds the program will wait for a
response before timing out</tooltip>
        <type>Integer</type>
        <uiOrder>5</uiOrder>
        <default>5</default>
        <min>1</min>
        <max>10000</max>
      </property>
    </group>
  </tab>
</velocityProperties>
```

```
ping $ip_address count $count size $packed_size interval $interval
timeout $timeout
```

Code 38-3: Sample OmniSwitch traceroute script

```
<velocityProperties>
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the host whose route you want to trace.
(IPv4 xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>maxHopValue</name>
        <uiName>Maximum Hop:</uiName>
        <tooltip>Maximum hop count for the trace</tooltip>
        <type>Integer</type>
        <default>5</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
    </group>
  </tab>
</velocityProperties>

traceroute $ip_address max-hop $maxHopValue
```

9 Perform one of the following.

a Save the script to the script manager.

i Choose File→Save from the Editor menu or click on the Save button. The Comment form opens.

ii Configure the parameters:

- Network Element Version Information
- Bundle ID

iii Click on the OK button.

b Export the script to a local or network text file.

i Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network.

ii Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

iii Click on the Export button. The script version text file is saved in the specified location.

10 Choose File→Close from the Editor menu. The Script Editor form closes, and the CLI Script (Edit) form reappears with the Version tab displayed. The new version of the script appears in the list.

11 Close the CLI Script (Edit) form.

12 Close the Script Manager list form.

See procedures 38-40 and 38-41 for information about configuring and running OmniSwitch ping and traceroute OAM scripts.

Procedure 38-39 To configure an advanced loopback test on an OmniSwitch port

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

Note 1 — Only one test profile per port can be created, up to a maximum of 8 ports on an NE.

Note 2 — The test profile cannot be created on a port that is part of a LAG.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device where you want to configure an advanced loopback test and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

5 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

6 Click on the Advanced Loopback tab button. Click on the Create button. The AOS Advanced Loopback (Create) form appears.

7 Configure the parameters:

- Test Name
- Source MAC Address
- Destination MAC Address
- VLAN
- Traffic Type
- SAP Id (OS 6250 only, see Note 1 and Note 2)

Note 1 — For OS 6250 NEs, if the Traffic Type parameter value is "Outward", the user will be provided with an option to specify the SAP Id, provided the SAP Id already exists on the NE.

Note 2 — If a loopback profile is created with a Traffic Type value of "Outward", the SAP Id option will be provided with the default value of "0". If the loopback profile is created with SAP Id, then the SAP Id must exist on the NE.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The AOS Advanced Loopback (Create) form closes.

10 Choose a test entry on the Physical Port (Edit) form. Click on the Apply button.

11 A dialog box appears. Click on the Yes button.

12 Choose a test entry on the Physical Port (Edit) form. Click on the Properties button.

13 The AOS Advanced Loopback (Edit) form opens. Configure the Status parameter.

14 Click on the OK button. The AOS Advanced Loopback (Edit) form closes.

15 Click on the OK button of the Physical Port (Edit) form. A dialog box appears.

16 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 38-40 To configure and run an OmniSwitch OAM ping

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch ping test using the script created using Procedure 38-38.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 14-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Script Manager form.

5 Double-click on the OmniSwitch ping script that you created using Procedure 38-38. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab button.

7 Click on the Create button. The Target Configuration form opens.

8 Click on the Create button. The Select Network Elements form opens.

9 Choose one or more OmniSwitch devices and click on the OK button. The Select Network Elements form closes, and the OmniSwitch nodes are listed on the Target Configuration form.

10 Configure the test parameters.

i Choose a target from the Target List panel.

ii Configure the parameters:

- IP Address
- Count
- Packet Size (octets)
- Interval (seconds)
- Timeout

iii Click on the Apply To Selected button.

iv Repeat steps 10i to 10iii to configure additional targets, if required.

v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) form opens with the Targets tab displayed.

11 To run the script on specified targets, choose one or more entries from the list.

12 Click on the Execute button. The results of the test appear in the form.

13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.

Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Script Manager form.

Procedure 38-41 To configure and run an OmniSwitch OAM traceroute

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch traceroute using the script created using Procedure 38-38.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 14-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager list form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Script Manager form.

5 Double-click on the OmniSwitch traceroute script that you created using Procedure 38-38. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab button.

7 Click on the Add button. The Target Configuration form opens.

8 Click on the Add button in the target list to add an OmniSwitch to the list. The Select Network Elements form opens with a list of OmniSwitch nodes.

9 Choose one or more OmniSwitch nodes and click on the OK button. The Select Network Elements form closes, and the OmniSwitch nodes appear in the target list panel of the Target Configuration form.

10 Configure the test parameters.

  i Choose a target from the Target List panel.

  ii Configure the parameters:

  - IP Address
  - Maximum Hop

  iii Click on the Apply To Selected button.

  iv Repeat steps 10i to 10iii to configure additional targets.

  v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) appears with the Targets tab displayed.

11 To run the script on the specified targets, choose one or more entries from the list.

12 Click on the Execute button. The test results appear.

13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.

Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Script Manager form.

Procedure 38-42 To configure an 802.3ah EFM OAM diagnostic

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- EFM OAMPDU tunneling
- high-resolution EFM OAM timers

The 5620 SAM supports EFM OAM diagnostic configuration on Ethernet ports in network mode on the 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

For OmniSwitch NEs, see Procedure 38-43.

Caution — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.

Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure an 802.3ah EFM OAM diagnostic and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

5 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

6 Click on the 802.3ah tab button. The 802.3ah form opens.

7 Configure the parameters:

- Administrative State
- Tunneling
- Mode
- Transmit Interval
- Multiplier (Intervals)
- Received Remote Loopback Requests
- Set Remote Loopback
- Set Local Loopback
- Hold Time (s)

8 Click on the Apply button. A dialog box appears.

9 Click on the Yes button.

10 Click on the Resync button.

11 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 38-4, 38-5, and 38-6 describe the displayed information.

Table 38-4 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.

(1 of 2)

Parameter	Value	Description
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 38-5 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueToOam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface

(1 of 2)

Statistics	Displayed Value	Description
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

(2 of 2)

Table 38-6 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

12 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 38-43 To configure an 802.3ah EFM OAM diagnostic on an OmniSwitch at the NE or port level

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- high-resolution EFM OAM timers

The EFM OAM diagnostic is supported at the NE level or at the Ethernet port level on the Ethernet ports in network mode.

Caution 1 — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.

Caution 2 — Link OAM (802.3ah) is not supported on mirroring ports.

Caution 3 — When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.

Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

To configure Link OAM at the NE level, go to Step 1.To configure Link OAM and 802.3ah EFM OAM diagnostics at the port level, go to Step 6.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the OmniSwitch device where you want to configure an 802.3ah EFM OAM diagnostic and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on the Globals tab button.

5 Click on the 802.3ah tab button. The 802.3ah form opens.

6 Configure the parameters:

- Administrative Status
- Multiple PDU Count
- Statistics
- Log-history

7 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

8 Expand to the port level and click on a port object. The Physical Port (Edit) form opens with the General tab displayed.

9 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

10 Click on the 802.3ah tab button. The 802.3ah form opens.

11 Configure the parameters:

- Administrative State
- Mode
- Transmit Interval
- Received Remote Loopback Requests
- Set Local Loopback
- Set Local Loopback
- Hold Time (s)
- Dying Gasp Notify
- Critical Event Notify
- Statistics
- Log-history
- Errored Frame Window (dsec)
- Errored Frame Period Window (frames)
- Errored Frame Seconds Summary Window (dsec)
- Threshold (frames)
- Period Threshold (frames)
- Seconds Summary Threshold (framesec)
- Notify
- Period Notify
- Seconds Summary Notify
- Number of Frames
- Frames Delay (ms)
- Start L1-Ping

12 Click on the Apply button. A dialog box appears.

13 Click on the Yes button.

14 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 38-7, 38-8, and 38-9 describe the displayed information.

Table 38-7 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.

(1 of 2)

Parameter	Value	Description
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 38-8 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueToOam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

Table 38-9 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

15 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 38-44 To view OAM diagnostic test results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Navigate to the test results.

The navigation path is Result (Assurance)→Test Result (Assurance). The ActionResult (Assurance), Ping Result (Assurance), and Trace Result (Assurance) objects contain the test results.

3 Select a filter option. Use the configurable filters choices and properties options on the Service Test Manager form and click on the Search button. The list of test results that meet the filter criteria are displayed.

4 Choose a test result from the list and click on the Properties button. The appropriate OAM diagnostic test results form opens with the General tab displayed.

5 Click on the form tabs to view the test results for the OAM diagnostic. You can click on the View button beside an object and open the properties form for the object.

a CFM Continuity Check OAM diagnostic information includes:

- identifies the MD and MEG involved in the test
- MEP creation on a SAP
- MEP creation on a SDP
- intervals (seconds) between continuity checks
- MHF creation

b CFM loopback OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- data size
- VLAN priority
- number of messages sent

c CFM link trace OAM diagnostic information includes:

- originating node
- originating MEP
- target MAC addresses
- TTL

d CFM One Way OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- priority

e CFM Two Way OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- VLAN priority

f CFM Single Ended Loss OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- test duration, in seconds
- number of LMR frames received
- number of frames transmitted by the far end
- number of frames received by the near end
- number of frames lost at the near end
- percentage of frames lost at the near end
- number of frames transmitted by the near end
- number of frames received by the far end
- number of frames lost at the far end
- percentage of frames lost at the far end

g CFM Eth Test OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- data size
- VLAN priority

h CFM Two Way SLM diagnostic information includes:

- Global Maintenance Entity Group
- Originating MEP

i MTU ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating tunnel ID
- administrative and operational states
- information about previous diagnostics, including the start and finish sizes of the MTU datagram (packet)
- ID of the service being diagnosed
- name of the service being diagnosed
- MTU response size, indicating the largest packet size that the tunnel can transport

j Tunnel ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating and return tunnel IDs
- administrative state
- operational state
- probes to be issued information
- message size
- forwarding class used by the service
- ID of the service being diagnosed
- name of the service being diagnosed
- average, minimum, and maximum one-way time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

k VPRN ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- inner and outer encapsulation value of the SAP supporting the requested ping response, when the address type is a SAP and in the case that the inner encapsulation value is from a 5620 SAM-managed device

l VPRN trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses

m VPRN ICMP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

n VPRN ICMP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target IP addresses
- operational size
- number of responses
- initial and maximum time to live
- time to wait (microseconds)

o MAC ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation

p MEF MAC Ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target MAC address
- service ID and name
- number of probes to be issued
- round trip jitter
- round trip latency
- round trip frame Loss

q MAC trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics

r Service site ping OAM diagnostic information includes:

- target and source IP addresses
- service ID and name
- probes to be issued information
- check mark buttons to specify whether a local tunnel, remote tunnel, or local and remote tunnel is performed
- information about previous service site OAM diagnostics, including probes sent and responses received, loss percentage, packet timeouts, and last good packet time
- ID of the service being diagnosed

s VCCV ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- IP address of the destination and far-end devices
- time of last response
- number of responses received
- response time
- loss indicator, with a value of 0 indicating that the test packet was received and a value of 1 indicating that the test packet was lost
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

t VCCV trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from nodes in path

u LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

v P2MP LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- test probe: size, Time to Live, Forwarding Class, Forwarding Profile
- results: probes sent, responses received, probe timeouts, probes lost
- probe result status
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

w P2MP LSP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- trace attempt: size, Initial Time to Live, Forwarding Class, Forwarding Profile
- probe result status
- number of probes sent
- responses received
- timeouts
- failures
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

x LDP Tree Trace Result diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number and IP address of hops included in the test
- destination IP address of the path associated with the hop
- next hop IP address
- a display of available hops in a tree format

y Multicast router OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- status of diagnostic
- number of sent, received, and lost packets
- packet loss percentage
- number of packet timeouts
- time for last successful contact with the target IP address

z Multicast trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and group multicast addresses
- destination and response IP addresses
- virtual router ID
- number of hops in path
- response from nodes in path
- number of trace attempts
- number of successful traces
- time for last successful trace
- identifier if multicast path changed from last successful trace

aa Multicast FIB ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

ab ICMP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- virtual router ID
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

ac ICMP trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and target IP addresses
- virtual router ID
- number of hops
- probe responses from managed devices
- number of trace probe attempts
- number of successful traces
- time for last successful trace
- initial and maximum time to live values

ad DNS ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- the IP Address for the requested DNS name, as reachable by the DNS server, shown for IPv4 addresses in dotted-decimal format
- status, including response received to indicate a successfully completed diagnostic

ae ANCP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- administrative and operational states
- ID of the circuit being diagnosed
- information about previous ANCP OAM diagnostics, including packet history size, probes sent and responses received, and packet failure

Procedure 38-45 To interpret OAM diagnostic results

1 Perform the OAM diagnostic, as described in Procedure 38-1 to Procedure 38-33.

2 Perform Procedure 38-44 to view OAM diagnostic test results.

3 The General and Response Packets tabs display the key information about OAM diagnostic results. When there is no packet information required, as for an OAM ping, the information appears on the Packets Results form without any tab buttons. For example, status and return code information appears directly on the Packets Results form. You can view test packet information by performing the following actions:

i Click on the Response Packets tab button. A list of test objects appears.

ii Choose an object from the display and click on the Properties button. The Packets Results form opens.

4 Interpret the results, based on the status and return code information.

a For MTU OAM diagnostics, the key information is how many frames were sent and incrementally increased in size before the frames could not be sent. When the frame cannot be sent because it is too large, that results in a request timeout message. The largest frame that was sent is the last frame size with an associated success response.

b For tunnel OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 38-10 lists the displayed messages and descriptions.

Table 38-10 Tunnel OAM diagnostics results

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is operationally down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is down.
Request Terminated	The operator terminated the request before a reply could be received or before the timeout of the request could occur.
Far End: Originator-ID Invalid	The request was received by the far end, but the far end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is down.
Success	The tunnel is in service and working as expected. A reply was received without any errors.

c For service site OAM diagnostics, the key information is the result of the diagnostic, which is displayed in the status message and with the other records from the General tab.

As the diagnostic traverses the service across the originating and destination IP addresses, the service tunnels, and the used VCs, the status of each portion of the service is displayed. Table 38-11 lists the displayed messages and descriptions.

Table 38-11 Service site OAM diagnostics results

Displayed message	Description
Sent - Request Timeout	The request timed out with a reply.
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.
Sent - Reply Received	The request was sent and a successful reply message was received.
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.
Not Sent - Non-Existent SDP for Service	There is no SDP for the service being tested.
Not Sent - SDP For Service Down	The SDP for the service is down.
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and responder.

d For MAC, VPRN, and multicast FIB ping OAM diagnostics, the key information is the result of the diagnostic. Table 38-12 lists the displayed messages, the return code, and descriptions.

Table 38-12 MAC, VPRN, multicast FIB ping OAM diagnostics results

Displayed message (return code)	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.

(1 of 2)

Displayed message (return code)	Description
tlvNotUnderstood (9)	One or more TLVs were not understood.
downstreamNotInMFib (10)	The replaying router is a downstream router, but it is not part of the MFIB.
Downstream mapping mismatched (11)	The downstream mapping is mismatched.
Upstream interface index unknown (12)	The upstream interface index is unknown.
Label switched but no MPLS forwarding at stack-depth (13)	The label switched successfully but MPLS forwarding did not occur at stack-depth.
No label entry at stack-depth (14)	The label entry at stack-depth did not occur.
Protocol not associated with interface at FEC stack-depth (15)	The protocol is not associated with the interface at FEC stack-depth.
Premature termination of ping due to label stack shrinking to a single label (16)	The ping was terminated prematurely due to the label stack shrinking to a single label.

(2 of 2)

e For multicast router OAM diagnostics, the key information includes information that is related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

f For multicast trace OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 38-13 lists the displayed messages and descriptions.

Table 38-13 Multicast trace OAM diagnostics results

Displayed message	Description
No Error	No error.
Wrong Interface	The router not forwarding the multicast source or group traffic because the router is not part of the multicast path.
Prune Sent	The router sent a prune request upstream that impacts the multicast source and group in the trace request.
Prune Received	The router stopped forwarding traffic for the multicast source and group in response to a request from the next hop router.
Scoped	The multicast group is subject to administrative scoping.
No Route	The router has no route for the multicast source or group and no way to determine a potential route.
Wrong Last Hop	The router is not the correct last-hop router.
Not Forwarding	The router is not forwarding the multicast source or group traffic for an unspecified reason.
Reached RP or Core	Request arrived on the rendezvous point or core.
Request on RPF	The request arrived on the expected RPF interface.
No Multicast	The request arrived on an interface that is not enabled for multicast traffic.
Hops Hidden	One or more hops are hidden from the trace.
Fatal Error	Fatal error.
No Space	There is insufficient room to insert another response data block in the packet.
Old Router	The previous router hop cannot process the multicast trace request.
Admin. Prohibited	The multicast trace was administratively prohibited.
Unknown	—

g For most diagnostics, some common return codes are used. The return codes indicate the status of OAM tests, usually when there was a problem performing the test. Table 38-14 lists the messages, return codes, and descriptions.

Table 38-14 OAM diagnostics return codes

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
unknown (2)	The OAM diagnostic failed for an unknown reason.
internalError (3)	An internal error on the device caused the diagnostic to not be performed.
maxConcurrentLimit Reached (4)	The device cannot perform the OAM diagnostics because there are too many OAM diagnostic operations already running.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.
unknownSDPOrigin (6)	Indicates an invalid or non-existent originating service tunnel.
downOrigSdpId (7)	The originating service tunnel is operationally down.
requestTerminated (8)	The OAM diagnostic was cancelled before the timeout or reply period was reached.
invalidOriginatorId (9)	The far-end device replied indicating that the originating ID was invalid.
invalidResponderId (10)	The far-end device replied with an invalid responding ID.
unknownRespSdpId (11)	The far-end device replied with an invalid response service tunnel ID.
downRespSdpId (12)	The responding service tunnel with the given ID is operationally or administratively down.
invalidServiceId (13)	An invalid or non-existent service ID.
invalidSdp (14)	An invalid or non-existent service tunnel for the service.
downServiceSdp (15)	The service tunnel bound to the service is down.
noServiceEgressLabel (16)	The egress label for the service does not exist.
invalidHostAddress (17)	The IP address for the host is invalid, for example, in the case of a broadcast or multicast IP address.
invalidMacAddress (18)	The MAC address specified in the OAM diagnostic is invalid.
invalidLspName (19)	The LSP name specified in the OAM diagnostic is invalid.
macIsLocal (20)	The MAC address is the local SAP or device MAC address, not the MAC address of the downstream SAP or device, therefore the MAC ping or trace cannot be sent.
farEndUnreachable (21)	No route is available to the far-end GRE service tunnel.
downOriginatorId (22)	The originating ping device is operationally down.
downResponderId (23)	The device responding to the ping is operationally down.
changedResponderId (24)	The ID of the device responding to the ping has changed.
downOrigSvcId (25)	The originating service identified by the ID is operationally down.
downRespSvcId (26)	The service responding to the ping identified by the ID is operationally down.
noServiceIngressLabel (27)	The ingress label for the service does not exist.
mismatchCustId (28)	The subscriber ID identified with the service differs from the originating device compared to the responding device.
mismatchSvcType (29)	The service type identified with the service differs from one device to another.
mismatchSvcMtu (30)	The service MTU size associated with the service differs from the originating device compared to the responding device.
mismatchSvcLabel (31)	The service label identified with the service differs from the originating device compared to the responding device.

(1 of 4)

Displayed message (return code)	Description
noSdpBoundToSvc (32)	There is no service tunnel bound to the service.
downOrigSdpBinding (33)	The service tunnel associated with the originating device's service is operationally down.
invalidLspPathName (34)	The LSP path name specified in the OAM diagnostic is invalid.
noLspEndpointAddr (35)	There is no LSP endpoint address specified in the OAM diagnostic.
noActiveLspPath (36)	There is no active LSP path.
downLspPath (37)	The far end of the LSP is operationally down.
invalidLspProtocol (38)	The LSP protocol is not valid or is not supported.
invalidLspLabel (39)	The LSP label is invalid.
routeIsLocal (40)	For a VPRN ping, the route is a local route.
noRouteToDest (41)	For a VPRN ping, there is no route available to the destination of the OAM diagnostic.
localExtranetRoute (42)	For a VPRN ping, the route is a local extranet route.
srcIpInBgpVpnRoute (43)	For a VPRN ping, the source IP address belongs to a BGP VPN route.
srcIpInvalid (44)	For a VPRN ping, the source IP address is invalid or no route is available to the source IP address.
bgpDaemonBusy (45)	For a VPRN trace, the BGP routing process is busy on the device, and VPRN route target information cannot be retrieved.
mcastNotEnabled (46)	Multicast is not enabled on the device, so the diagnostic cannot be performed.
mTraceNoSGFlow (47)	—
mTraceSysIpNotCfg (48)	The system IP address is not configured. The address is required for a response to a multicast trace.
noFwdEntryInMfib (49)	No forwarding entry could be found for the specified source and destination addresses in the MFIB.
dnsNameNotFound (50)	The domain name specified in the dns query does not exist
noSocket (51)	For icmp-ping, unable to get socket.
socketOptVprnIdFail (52)	For icmp-ping, unable to set SO_VPRNID for socket.
socketOptIfInexFail (53)	For icmp-ping, unable to set IP_IFINDEX for socket.
socketOptNextHopFail (54)	For icmp-ping, unable to set IP_NEXT_HOP for socket.
socketOptMtuDiscFail (55)	For icmp-ping, unable to set IP_MTU_DISC for socket.
socketOptSndbufFail (56)	For icmp-ping, unable to set SO_SNDBUF for socket.
socketOptHdrincFail (57)	For icmp-ping, unable to set IP_HDRINCL for socket.
socketOptTosFail (58)	For icmp-ping, unable to set IP_TOS for socket.
socketOptTtlFail (59)	For icmp-ping, unable to set IP_TTL for socket.
bindSocketFail (60)	For icmp-ping, unable to bind socket.
noRouteByIntf (61)	For icmp-ping, no route to destination via the specified interface.
noIntf (62)	For icmp-ping, no interface specified.
noLocalIp (63)	For icmp-ping, unable to find local ip address.
sendtoFail (64)	For icmp-ping, sendto function failed.

(2 of 4)

Displayed message (return code)	Description
rcvdWrongType (65)	For icmp-ping, received packet of wrong icmp type.
noDirectInterface (66)	For icmp-ping, no direct interface to reach destination.
nexthopUnreachable (67)	For icmp-ping, unable to reach the next-hop.
socketOptHwTimeStampFail (68)	For icmp-ping, unable to set IP_TIM_TIME for socket.
noSpokeSdpInVll (69)	For vccv-ping, unable to find spoke-sdp given SdpId:vc-id
farEndVccvNotSupported (70)	For vccv-ping, far end does not support the VCCV options.
noVcEgressLabel (71)	For vccv-ping, no Vc egress label to send vccv-ping
socketOptIpSessionFail (72)	For icmp-ping, unable to set IP_SESSION for socket.
rcvdWrongSize (73)	For icmp-ping, received packet of wrong size.
dnsLookupFail (74)	For icmp-ping, dns lookup failed.
noIpv6SrcAddrOnIntf (75)	For icmp-ping, no ipv6 source on the interface.
multipathNotSupported (76)	For lsp-trace, downstream node does not support multipath.
nhIntfNameNotFound (77)	For lsp-ping/trace, Given next-hop interface name not found.
msPwInvalidReplyMode (78)	For vccv-ping, MS-PW switching node supports ip-routed reply mode only.
ancpNoAncpString (79)	ANCP string unknown to the system.
ancpNoSubscriber (80)	Subscriber unknown to the system.
ancpNoAncpStringForSubscriber (81)	Subscriber has no associated ANCP string.
ancpNoAccessNodeforAncpString (82)	No access node is found for the given ANCP string.
ancpNoAncpCapabilityNegotiated (83)	ANCP capability not negotiated with the involved DSLAM.
ancpOtherTestInProgress (84)	Another ANCP test is running for this ANCP string.
ancpMaxNbrAncpTestsInProgress (85)	Maximum number of concurrent ANCP tests reached.
spokeSdpOperDown (86)	For vccv-ping, spoke-sdp is operationally down.
noMsPwVccvInReplyDir (87)	Switching node in MS-PW with no vccv support in echo reply direction.
p2mpLspNameOrInstInvalid (88)	P2MP LSP name or instance provided is not valid.
p2mpLspS2LPathDown (89)	LSP path to S2L is down.
p2mpLspS2LAddressInvalid (90)	One or more S2L address is not valid.
p2mpLspNotOperational (91)	P2MP LSP is operationally down.
p2mpLspTrMultipleReplies (92)	Probe returned multiple responses. Result may be inconsistent.
invalidMepId (93)	The user-configured MEP identifier is not valid.
multipleReplies (94)	More than one reply received, when one was expected.
packetSizeTooBig (95)	Packet size is too big.
gtpPingError (96)	General GTP Ping Error.
gtpPingRsrcUnavailable (97)	GTP Path management resource unavailable.
gtpPingDupRequest (98)	Duplicate request for the same peer.

(3 of 4)

Displayed message (return code)	Description
gtpPingCleanUpInProg (99)	GTP Path management clean up in progress.
invalidInterface (100)	The egress interface specified does not exist.

(4 of 4)

Procedure 38-46 To configure threshold-crossing alarms on NE-schedulable OAM tests

You can configure threshold-crossing alarms for OAM tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

You can also configure threshold-crossing alarms on test definitions within a test policy. See Procedure 78-6 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose an NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the Threshold Alarms tab.

7 Click on the Create button. The NE Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

9 Click on the Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NE Threshold Event (Create) form closes.

14 Repeat steps 7 to 13 to configure threshold events on additional tests.

15 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

16 Close the Test (Edit) form. The Service Test Manager form reappears.

17 Close the Service Test Manager form.

Procedure 38-47 To configure NM threshold-crossing alarms on non-NE-schedulable OAM tests

You can configure NM threshold-crossing alarms for OAM tests that are non-NE-schedulable. NM threshold-crossing alarms are not configurable for service site ping, VPRN trace, MTU ping, Mrinfo and Mtrace tests. An alarm is raised when an NM threshold is crossed, either because the value rose above or fell below the configured level. The type of NM threshold-crossing event available for selection depends on the test type.

Non-NE-schedulable OAM tests can be configured as NE persistent. NE persistent tests are deployed to the network node after the first execution and remain on the node each time the test is executed.

You can also configure NM threshold-crossing alarms on test definitions within a test policy. See Procedure 78-7 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose a non-NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the NM Threshold Alarms tab.

7 Click on the Create button. The NM Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

Note — If you are configuring an NM threshold-crossing alarm for an NE persistent test, the type of NM threshold-crossing event available for configuration depends on the test type.

9 Click on the NM Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the NM Falling Threshold tab.

Note — The NM Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NM Threshold Event (Create) form closes, and a dialog box appears.

14 Click on the OK button.

15 Click on the Apply button on the Test (Edit) form. A dialog box appears.

16 Confirm the action. The test appears on the list.

17 Repeat steps 7 to 16 to configure NM threshold events on additional tests.

18 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

19 Close the Test (Edit) form. The Service Test Manager form reappears.

20 Close the Service Test Manager form.

Procedure 38-48 To edit an OAM diagnostic test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4. Click on the Search button. A list of tests is displayed.
5. Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.
6. Change any configurable parameter for the test.
7. Click on the OK button to save the changes. A dialog box appears.
8. Confirm the action. The modified test or tests are shown in the list.

Procedure 38-49 To delete an OAM diagnostic test

1. Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.
2. Choose Test (Assurance) icon from the object drop-down list.
3. Configure the filter criteria.
4. Click on the Search button. A list of tests is displayed.
5. Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.
6. Choose one or more OAM diagnostic tests from the results list and click on the Delete button. A dialog box appears.
7. Confirm the action. The test or tests are deleted from the list of available OAM diagnostic tests.

Procedure 38-50 To set STM managed device test limits

You can configure the maximum number of pings and traces allowed to be performed from the 5620 SAM by the managed devices, or you can limit the number of tests performed. The default is to allow an unlimited number of tests.

Note 1 — You must enable debug STM mode before you perform this procedure. See Procedure 78-3 for more information.

Note 2 — Limiting the number of tests does not raise an alarm on 5620 SAM or an SNMP trap on the managed device. The indication that the limit has been reached is no returned test results.

1. Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.
2. Choose NE Test Agent (Assurance) from the object drop-down list.
3. Click on the Search button. A list of NE Test Agent policies appears, one for each managed device.

4 Choose on one or more policies from the list and click on the Properties button. The configuration form opens.

5 You can set the number of tests allowed for individual managed devices, or for all managed devices, using the following parameters:

- Unlimited Concurrent Pings
- Unlimited Concurrent Traces
- Maximum Concurrent Pings
- Maximum Concurrent Traces

6 Click on the Apply button to save the changes. A dialog box appears.

7 Click on the Yes button to confirm the action.

39 — VRRP

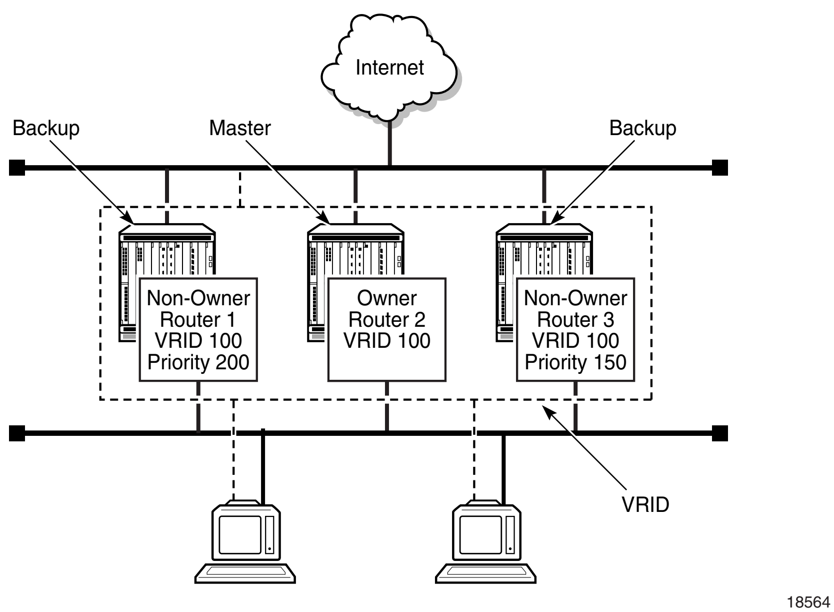
39.1 VRRP overview

The 5620 SAM supports VRRP management. VRRP creates a redundant routing system that takes over packet transmission on a common LAN segment when a router fails. VRRP designates alternative routing paths in the form of virtual routers, or VRs, without changing the IP or MAC address of a protected router.

A VRRP protected router owns the IP address of the VR. The VRRP owner forwards packets using the default gateway. When the owner router fails, packet-forwarding responsibilities are transferred to a designated backup router. This router becomes the master and forwards packets using the VR IP address.

Figure 39-1 shows a basic VR that acts in parallel with the real network. Router 2 is the owner with the address from which packets are forwarded. If Router 2 fails, Router 3, which has been configured to route using the master address in a backup role, begins to forward packets using this IP address. Router 1 is also a backup router, but because its priority number is higher, it ranks below Router 3.

Figure 39-1 VR concepts

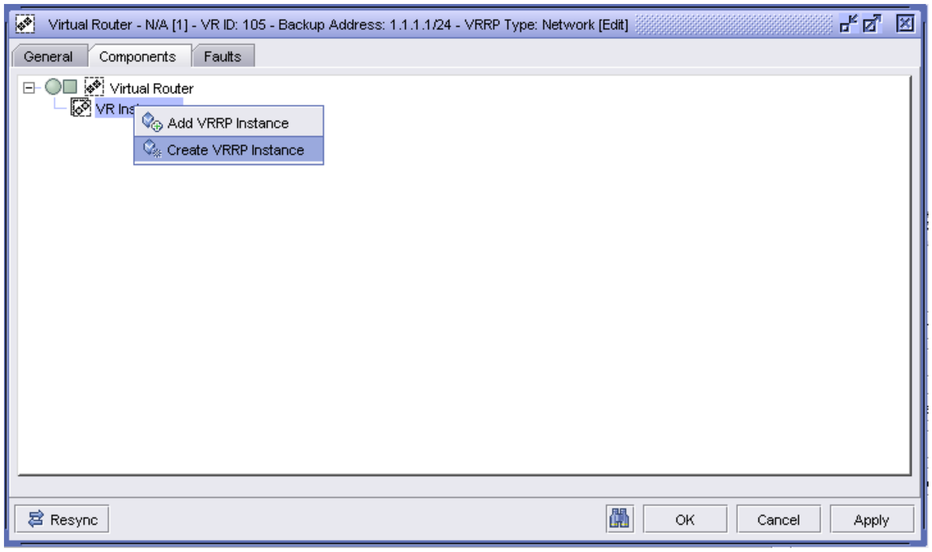


The 5620 SAM supports the configuration of VRs for network interfaces and for L3 access interfaces.

VRRP in an IES involves interfaces from separate IESs. VRRP in a VPRN requires interfaces that are in the same VPRN service. The 5620 SAM supports on-demand, but not scheduled, statistics collection for VRRP in a VPRN. Certain VRRP SNMP traps do not apply to VPRN; see the appropriate NE documentation for information.

You can configure the VR through another set of tabbed forms and a navigation tree, which allows you to add VRRP instances IP owner and non-owner router interfaces, as shown in Figure 39-2.

Figure 39-2 Adding or creating a VRRP instance

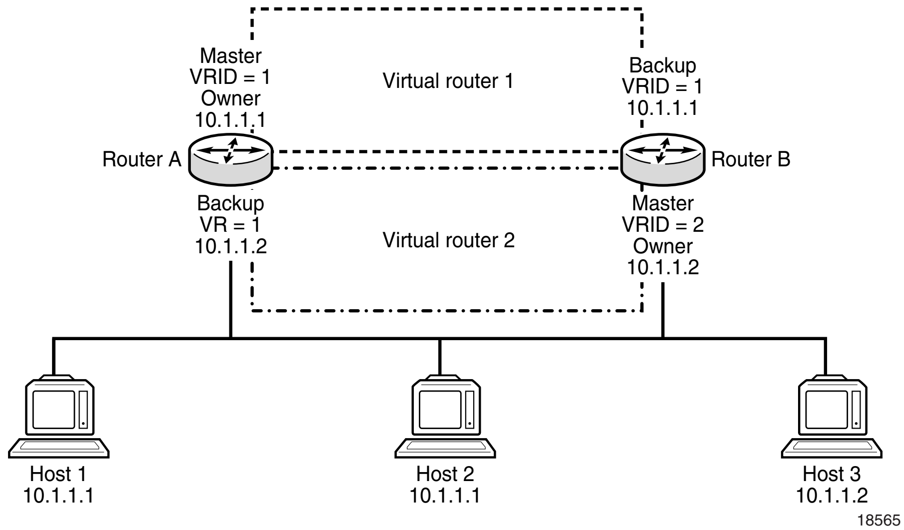


VR

A VR is a logical entity, managed by VRRP, that acts as a default router for hosts on a shared LAN. The VR consists of a VRID and a subnet (that is, ip_address/mask). A VRRP router can back up one or more VRs. The purpose of supporting multiple IP addresses in a single VR is for multi-netting. This common mechanism allows multiple local subnet attachments on a single routing interface. Up to four VRs are allowed on a single Alcatel-Lucent IP interface. The VRs must be in the same subnet.

Figure 39-3 shows a common VR setup in which associated routers provide mutual backup using VRRP. Router A forwards packets on IP address 10.1.1.1 to Hosts 1 and 2 on its default gateway. Router B forwards packets on IP address 10.1.1.2 to Host 3 on its default gateway. If Router A fails, VRID 1 uses IP address 10.1.1.1 to forward packets from Router B to Hosts 1 and 2. At the same time, the Router B interface is still configured to deliver packets on IP address 10.1.1.2 to Host 3. If Router B fails, VRID 2 forwards these packets through backup Router A.

Figure 39-3 Sample VRs



Master router

The VRRP master router, in either a normal or a failover situation, routes all IP packets into the LAN using the physical MAC address for the IP interface as the Layer 2 source MAC address. ARP packets also use the parent IP interface MAC address as the Layer 2 source MAC address.

Owner and non-owner VRRP instances

A VRRP instance is configured in either an owner or non-owner mode.

The owner instance controls the IP address of the VR and is responsible for forwarding packets sent to this IP address. The IP address of the owner VRRP instance is the same as the real interface IP address of the router. The owner assumes the role of the master VR when it is functioning normally in the network. Only one VRRP instance in the domain is configured as the owner. All other instances participating in the domain are non-owners and must have the same VRID.

A backup router becomes the master router after a failover and continues to use the IP address of the original master. As a result, the new master router is the IP address non-owner.

The most important parameter to define for a non-owner VRRP instance is the priority. The priority defines for a VR the selection order. The priority value and the preempt mode combine to determine which VR has the highest priority and becomes the master.

The base priority is used to derive the in-use priority of the VRRP instance as modified by an optional VRRP priority-control policy. VRRP priority-control policies are used to either override or adjust the base priority value depending on events or conditions in the node. See chapter 51 for more information.

VRRP types

When you create a VR, you specify the VRRP type, for example, network or L3 service, and the VR instance is restricted to the specified VRRP type. Configuring a VR using a mix of network and service interfaces through CLI raises a configuration mismatch alarm.

Primary addresses

A primary IP address is an address that is selected from the set of real interface addresses on the VR. VRRP advertisements between master and backup VRRP instances are sent using the primary IP address as the source of the IP packet.

The 7450 ESS or 7750 SR IP interface must always have an assigned primary IP address for VRRP to operate on the interface. The primary IP address of the VR and the primary address on the IP interface are always the same.

Backup addresses

A maximum of 16 IP addresses (for either IPv4 or IPv6) in different subnets can be configured for a VRRP instance. One backup address is permitted for a subnet. The number of backup addresses is limited to the number of primary and secondary addresses configured on the IP interface.

The backup IP addresses for the owner VRRP instance must match the primary address or one of the secondary addresses on the IP interface. If the VRRP instance is not the owner, the backup addresses must be in the subnets of the primary and secondary addresses of the IP interface.

The 5620 SAM includes only eligible IP addresses in the search list.

VRRP message authentication

The type of authentication used by the VR in VRRP advertisement is specified during VRRP instance creation. The current master router uses the configured authentication type when sending VRRP advertisements to backup routers, which authenticate the messages.

39.2 Workflow to configure VRRP

1. Before you create a VR, ensure that a primary IP address is configured for the network or L3 service interface. Each interface must have a primary IP address. See Procedure 30-9 for more information.

2. Configure the VRRP priority-control policy for a non-owner VRRP instance. See chapter 51 for more information about VRRP priority-control policy events.

3. Create the VR. See Procedure 39-1 for more information.

4. As required, create VRRP instances in the VR. See Procedure 39-2 for more information.

39.3 VRRP management procedures

Use the following procedures to perform VR creation and VRRP management tasks.

Procedure 39-1 To create a VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Click on the Create button. The Virtual Router (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Virtual Router ID
- Backup Address
- Name
- Description
- VRRP Type
- Subnet Mask

If you are creating an IPv6 VR, the Backup Address parameter value that you specify must be an IPv6 address.

4 Click on the OK button. The Virtual Router (Create) form closes.

Procedure 39-2 To create and configure a VRRP instance

Before you create a VRRP instance on an interface, ensure that the L3 service or network interface is configured with a primary IP address. The backup IP address that is configured in Procedure 39-1 must belong to the same subnet as the primary IP address of the owner VRRP instance created in this procedure. The 5620 SAM automatically configures a backup address using the IP address of the VR. A search of interface IDs in step 7 of this procedure displays the interface IDs that are eligible for the creation of a VRRP instance for the VR.

You can configure up to a total of four VRRP instances (IPv4 plus IPv6) on one IP interface. However, only one IPv6 instance can be included in this total. The maximum number of mixed IPv4 and IPv6 VRRP instances on an NE is 1024.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Select and right-click on VR Instances and choose Create VRRP Instance from the contextual menu. The VRRP Instance (Create) form opens with the General tab displayed.

Note — If the Backup Address parameter value that you specified in step 3 of Procedure 39-1 is an IPv6 address, then the contextual menu item is Create VRRP IPv6 Instance, and the VRRP IPv6 Instance (Create) form opens.

6 Click on the Select button in the Interface panel. The Select Interface - VRRP Instance or Select Interface - VRRP IPv6 Instance form opens, depending on whether you are creating an IPv4 or IPv6 VRRP Instance respectively.

7 Use the configurable filter and Search button to choose an interface, and click on the OK button. The Select Interface - VRRP Instance (or Select Interface - VRRP IPv6 Instance) form closes and the VRRP Instance (Create) (or VRRP IPv6 Instance (Create)) form reappears with the interface information displayed.

8 Configure the parameters:

- Owner
- Administrative State
- Base Priority

9 If the Owner parameter in step 8 is set to true, you cannot configure the Administrative State and Base Priority parameters and you cannot associate a policy with this VRRP instance. Go to step 11.

10 Assign a VRRP policy to the instance, if required.

Note — The same VRRP policy can be applied to both IPv4 VRRP instances and IPv6 VRRP instances.

- Click on the Select button in the Policy panel. The Select VRRP Policy form opens.
- Choose a VRRP policy and click on the OK button. The Select VRRP Policy form closes and the VRRP Instance (Create) form reappears with the VRRP policy information displayed.

11 Click on the Behavior tab button.

12 Configure the parameters:

- MAC Address
- Message Interval (seconds)
- Message Interval (milliseconds)
- Init Delay (seconds)
- Master Inherit Interval
- Ping Reply
- Telnet Reply
- Standby Forwarding
- Preempt Mode
- SSH Reply
- Traceroute Reply

13 If you require bi-directional forwarding detection for the VRRP instance, configure the Enable BFD Interface parameter, and then complete the following substeps:

i Click on the BFD Interface tab button.

ii Click on the Select button next to the Sevice Name parameter and choose a service from the Select Service - BFD Interface window.

iii Click on the Select button next to the Interface Name parameter and choose a service from the Select Interface - BFD Interface window.

iv Configure the Destination Address parameter.

14 Click on the Authentication tab button.

Note — The Authentication Key is not supported for Release 7.0 R1 VRRP IPv6 Instances. If you are creating an VRRP IPv6 Instance on a Release 7.0 R1 NE, the Authentication tab is not displayed.

15 Configure the parameters:

- Type
- Init Delay (seconds)

16 Click on the Backup Addresses tab button.

17 Click on the Create button. The Backup Address (Create) form opens.

18 Perform one of the following to configure backup addresses:

a Enter an IPv4 address (for an IPv4 VR) or IPv6 address (for an IPv6 VR) manually in the IP Address field in the Backup Address section.

b Select the IP address from a list:

i Click the Choose IP Address button adjacent to the IP Address field. The Select IP Address form opens.

ii Click on the Search button.

iii Choose the desired entry from the list.

iv Click on OK.

The Select IP Address form closes and the IP Address parameter is populated with your selection.

v Click on the Add Link Local Address button. The Admin Link Local Address defined for the network L3 access interface appears in the IP Address field.

Note — If you need to add the Link Local Address as a backup address, then the Admin Link Local Address must be configured and the Admin Link Local Address Preferred parameter must be enabled for the network L3 access interface that you are using. See Procedure 30-7 for more information.

19 Click on OK to save your changes and close the Backup Address (Create) form.

20 Click on the OK button. The Virtual Router (Edit) form reappears with the VRRP instances displayed in the VR instances tree.

Procedure 39-3 To add a VRRP instance

A VRRP instance that you add to the VR must have an IP address with the same VRID and subnet as those of the VR.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on VR Instances and choose Add VRRP Instance.

> **Note —** If you chose an IPv6 VR in step 3, the contextual menu item is Add VRRP IPv6 Instance, and the Select VRRP IPv6 Instance form opens.

The Select VRRP Instance form opens with a list of eligible instances.

6 Select an instance and click on the OK button. The Select VRRP Instance (or Select VRRP IPv6 Instance) form closes and the Virtual Router (Edit) form reappears with the interface information displayed.

Procedure 39-4 To modify a VR or VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Configure the VR parameters.

To configure parameters for a VRRP instance, click on the Components tab, select and right-click on the VRRP instance, and choose Properties from the contextual menu. Using the contextual menu, you can also:

- Configure the NE associated with the VRRP instance
- Configure the interface associated with the VRRP instance

5. Click on the Properties button in the Instance panel. The VRRP Instance (Edit) form opens with the General tab displayed.

6. The following tabs list the VRRP instance properties that you can select and configure:

   - General—associations between the VRRP instance and NEs, network interfaces, and policies (non-owner VRRP instances only).
   - Behavior—a virtual MAC address that must be the same for all participating VRRP instances
   - Authentication—enables authentication of VRRP advertisements among participating VRRP instances in the VR. For more information, see "VRRP message authentication" in section 39.1.

   Note — Authentication is not supported for Release 7.0 R1 VRRP IPv6 Instances. When you modify a Release 7.0 R1 VRRP IPv6 Instance, the Authentication tab is not displayed.

   - Backup Addresses—lists backup addresses, whose configuration options you can access by selecting a site and clicking on the Properties button. For more information, see "Backup addresses" in section 39.1.
   - VR Instances—lists VRs, whose configuration options you can access by selecting a VR and clicking on the Properties button. For more information, see "Owner and non-owner VRRP instances" in section 39.1.

7. Modify the parameters for the VRRP instance as required.

8. Click on the OK button. A dialog box appears.

9. Click on the Yes button to confirm the action. The VRRP Instance (Edit) form closes and the VR Instance (Edit) form reappears.

10. Click on the Close button to close the VR Instance (Edit) form.

Procedure 39-5 To view the status of a VR

The status of a VR informs you of potential problems, such as problems involving VR preconditions and operational states. You can view the following virtual status information:

- Aggregated Operational State—indicates the collective operational states of the VRRP instances in the VR, such as whether all instances are up, all instances are down, or one or more is down
- Number Of VRRP Instances—the number of owner and non-owner VRRP instances in the current VR

- Multiple Owners configured—one owner for each VR
- VR Instance(s) Down—one or more VRs are not working
- Backup Address Mismatch—the backup address for a VRRP instance does not match the primary IP address of the owner, and so does not match the VR IP address
- Only one instance configured—only one VR instance exists, either a master or backup; both are required
- Subnet Mismatch—the IP addresses of the owner and non-owner routers do not belong to the same subnet
- No Owner configured—an IP address owner is not assigned to the current VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed. Status information is in the Status panel.

4 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 39-6 To delete a VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Select and right-click on a VR instance and choose Delete from the contextual menu. A dialog box appears.

6 Click on the Yes button to confirm the action. The VR is deleted and removed from the VR instances tree.

7 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 39-7 To delete a VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR from the list.

4 Click on the Delete button. A dialog box appears.

5 Click on the Yes button to confirm the action. The VR is removed from the list.

6 Click on the Close button to close the Manage VRRP Virtual Routers form.

40 — APS

40.1 APS overview

APS protects SONET/SDH lines from linear bidirectional failures. The NEs in a SONET/SDH network constantly monitor the health of the network. When a failure is detected, the network proceeds to transfer, or switch over, live traffic from the active, or working line, to the standby, or protection line. The transfer occurs quickly to minimize traffic loss. The traffic remains on the protection line until the fault on the working line clears, at which time the traffic can optionally revert to the working line.

In a 1+1 APS architecture, the active OC-*n* signal is transmitted to both the working and protection ports, so the same payloads are transmitted identically to the working and protection ports in the egress direction. The working and protection signals are selected independently in the ingress direction.

Caution — An NE transmits data only on the working line. For a single failure, this configuration can cause a delay of up to 100 ms during an APS switch.

In the 5620 SAM, the main APS elements are the following:

- APS groups

  An APS group is an aggregation of one or two SONET/SDH ports and the associated logical ports, known as APS channels. The first port is known as the working channel and must be configured in the APS group. The second port is the protection channel, which is optionally configurable. In a 1+1 optimized APS group, the protection channel is replaced with a second working channel.
- APS channels

  APS channels are logical and model the physical ports. The set of associated data for an APS channel includes the corresponding physical port identifier, the role, which is working or protection, and the name of the APS group to which the port belongs. If a protection channel is configured, it carries the traffic of the failed working channel. If the protection channel fails, the working channel carries the traffic.
- APS bundles

  APS bundles protect multilink PPP and IMA bundles on channelized ASAP MDAs. All the members of a working or protection APS bundle must belong to the same working or protection line of the APS group.
- APS common port configurations

  All SONET/SDH port parameters on the working and protection channels in an APS group must be identical except for the following:
  - Clock Source
  - Loopback
  - Report Alarms
  - BER Signal Degradation Threshold
  - BER Signal Failure Threshold
  - SONET Section Trace Mode

- APS commands

  Each APS channel has one APS operational command associated with it. The APS operational command is determined by the last command that is issued to both APS channels and the signal condition of the working and protection ports. APS commands affect the APS operational states but do not affect the configuration. The operational state does not persist through an NE restart.

Table 40-1 describes the events that affect 1+1 protection and their relative priority.

Table 40-1 Events affecting 1+1 protection

Priority	Event	Event type
1	Lockout of protection	User initiated
2	Signal failure on protection line	Automatically initiated
3	Forced switch	User initiated
4	Signal failure on working line	Automatically initiated
5	Signal degradation	Automatically initiated
6	Manual switch	User initiated
7	WTR time (revertive switching only)	User initiated (state request)
8	No reversion (non-revertive switching only)	User initiated (state request)

Consider the following when configuring APS.

- A port can belong to only one APS group.
- Two ports that belong to the same APS group must be of the same port type and have the same traffic speed.
- An APS group has one set of APS channels. The set can contain one or two APS channels.
- An APS channel can belong to only one APS group.
- A SONET/SDH port can either belong to only one APS channel.

Bidirectional mode

In 1+1 system bidirectional mode, a signal failure in either direction causes both the near-end and far-end NEs to switch to the protection channels. The highest-priority local request is compared with a remote request; the request that has the greater priority is selected. See Table 40-1 for the list of events that affect 1+1 protection.

Unidirectional mode

In a 1+1 system unidirectional mode, the working interface switches to the protection interface only for the direction in which a signal failure occurs. For example, if there is a signal failure in the transmit direction, the working interface switches to the protection interface for transmission but not for the receipt of data.

Switching modes

The following 1+1 system switching modes are available:

- non-revertive (default)
- revertive

In non-revertive switching, a switch to the protection channel is maintained even after the working line has recovered from a failure or a manual switch is cleared.

In revertive switching, the traffic is switched back to the working channel after the working line has recovered from a failure or a manual switch is cleared.

For revertive switching, you can define a period of time that the system must wait before it can restore traffic from the protection line to the working line. This delay, or WTR time, prevents frequent automatic switches from occurring as a result of intermittent failures.

In case of failure on both the working and protection lines, the line that has the less severe error remains active. If there is a signal degradation on both lines, the active line that failed last remains active. If there is a signal failure on both lines, the working line always remains active because a signal failure on the protection line is a higher priority than a signal failure on the working line.

MLPPP

MLPPP provides a way to distribute data across multiple links within an MLPPP APS bundle to achieve high bandwidth. MLPPP allows for a single frame to be fragmented and transmitted across multiple links. This reduces latency and allows for a higher maximum received recovery unit, or MRU.

MLPPP is supported in MC APS groups. See section “MC APS” for more information about MC APS.

Multiclass MLPPP

Multiclass MLPPP is an extension of the MLPPP standard which allows multiple classes of service to be transmitted over an MLPPP bundle.

Multiclass MLPPP changes the MLPPP header to include either two or four class bits to allow for up to either four or 16 classes of service. This allows multiple classes of services over a single MLPPP connection. The highest priority traffic is transmitted over the MLPPP bundle with minimal delay, regardless of the order in which packets are received.

Multiclass MLPPP is useful in mobile network deployments where multiple types of traffic, each with its own priority level, travel across a single MLPPP link bundle between the base station router and the aggregation router in the point of presence (POP) mobile operator.

Note — Multiclass MLPPP allows for several classes of services to be transmitted over an MLPPP bundle. Link fragmentation and interleaving, however, allows for only two classes of service to be transmitted. Multiclass MLPPP and link fragmentation and interleaving are mutually exclusive.

APS port configurations

A 7710 SR or 7750 SR network or access port can be connected to another 7710 SR or 7750 SR with both the working and protection channels on different IOMs in a single NE, or with the working channel on one NE and the protection channel on another.

Note — Mirroring parameters configured on a specific port or service are maintained during an APS failover.

All SONET/SDH MDAs support APS functionality. Table 40-2 lists the possible port pairings to provide APS protection. Both ports must be of the same type and have the same traffic speed.

Table 40-2 APS port configurations

MDA type—Working channel	MDA type—Protection channel
16 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
8 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
16 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
8 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
4 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
2 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
1 × OC192	1 × OC192
16 × ATM OC3 SFP	16 × ATM OC3 SFP
4 × ATM OC12/OC3 SFP	4 × ATM OC12/OC3 SFP
4 × Channelized OC3 ASAP	4 × Channelized OC3 ASAP
1 × Channelized OC12 ASAP	1 × Channelized OC12 ASAP
1 × Channelized OC3 CES	4 × Channelized OC3 CES
4 × Channelized OC3 CES	1 × Channelized OC3 CES
1 × Channelized OC12 CES	1 × Channelized OC12 CES

Note — The working and protection channels for the following MDA port pairs are set to the same traffic speed based on the APS group speed configuration:

- 16 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 16 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 4 × ATM OC12/OC3 SFP and 4 × ATM OC12/OC3 SFP

SC APS

1+1 APS can be implemented on a port-by-port basis. If all ports on an MDA or IOM need to be protected, the ports must be individually configured.

The working and protection lines are capable of being connected to:

- two ports on the same MDA
- two ports on different MDAs, and the MDAs are on the same IOM
- two ports on different MDAs on different IOMs

If the working channel and protection channel are on the same MDA, protection is limited to the physical port and the media that connect the two NEs. If different IOMs are used, protection extends to failure of each IOM.

Working and protection lines can be connected to a 7450 ESS, 7710 SR, or 7750 SR, and serve as an access port that provides one or more services to the NE. The access port can be a single channel or multiple channels; each channel must support PPP. In the case of the ATM MDA, each channel must support ATM.

The end NE transmits a valid data signal to both the working and protection lines. The signal on the protection line is ignored until the working channel fails or degrades to the degree that requires a switchover to the protection channel. When the switchover occurs, all services, including all service QoS and filter policies, are activated on the protection channel.

The working channel on a 7750 SR, 7450 ESS, or 7710 SR must connect to the working channel on a peer NE, and the protection channel on a 7750 SR, 7450 ESS, or 7710 SR must connect to the protection channel on a peer NE.

1+1 optimized

You can configure an SC APS group with a 1+1 optimized configuration. A 1+1 optimized APS group is optimized for networks which rely primarily on 1+1 bidirectional switching. A 1+1 optimized APS group is configured with two working channels, as opposed to one working channel and one protection channel. In a 1+1 optimized configuration, one working channel acts as the primary channel, through which the traffic will always default. A 1+1 optimized APS group always operates in bidirectional and nonrevertive modes.

MC APS

You can use APS to protect against NE failure by configuring the working channel of an APS group on one 7750 SR or 7710 SR, and configuring the protection channel of the same APS group on a different 7750 SR or 7710 SR. The two NEs connect using an IP link that is used to establish a signaling path between them.

The working channel on the near-end NE must connect to the working channel on a peer NE, and the protection channel on the far-end NE must connect to the protection channel on a peer NE.

When an MC APS group is configured, the 5620 SAM automatically creates a container which aggregates the MC APS group configurations of each NE.

Multi-chassis APS configuration is supported for ATM clear channel interfaces.

APS on channelized ASAP MDAs

You can protect a channelized SONET/SDH port on a channelized ASAP MDA with a protection port of the same speed on a different channelized ASAP MDA in the same NE. The APS configuration on a channelized ASAP MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized ASAP MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on channelized CES MDAs

You can protect a channelized SONET/SDH port on a channelized CES MDA with a protection port of the same speed on a different channelized CES MDA in the same NE. The APS configuration on a channelized CES MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized CES MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on multilink bundles

APS on multilink bundles consists of a working and protection bundle which provide bidirectional APS protection to each other. The members of a working or protection multilink bundle must belong to the same working or protection line of the APS group. User traffic is not sent on the protection line.

The 5620 SAM supports APS on MLPPP and IMA bundles. In IMA bundles, IMA cells are sent on the protection line as a keep-alive signal during an APS switchover.

APS 1+1 configuration on the channelized MDA provides protection to all the channels on the protected SONET/SDH port and to all of the multilink bundles with member that links reside on the protected SONET/ SDH port.

APS bundles on multiple NEs

You can configure APS bundles to provide bidirectional APS protection across multiple NEs. MC APS bundles are supported on the 7750 SR and 7710 SR.

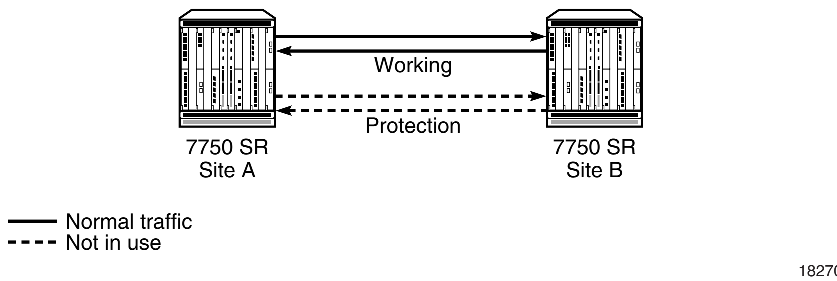
You can use APS to protect against failure by configuring the working bundle on one NE, and configuring the protection bundle of the same APS bundle group on a different NE. The two NEs connect to each other with an IP link that is used to establish a signaling path between them.

1+1 APS configuration example

Figures 40-1 and 40-4 show an example of 1+1 APS for two 7750 SRs that are configured for 1+1 APS in bidirectional and non-revertive modes.

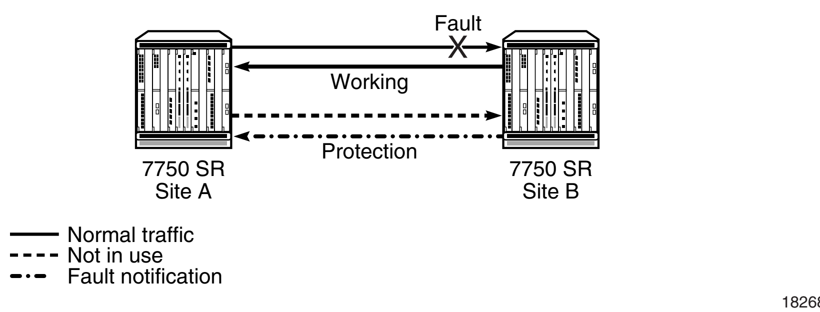
Figure 40-1 shows normal operations between two 7750 SRs. There are no faults on the working line, and the protection line is not in use.

Figure 40-1 Normal operations between two 7750 SRs



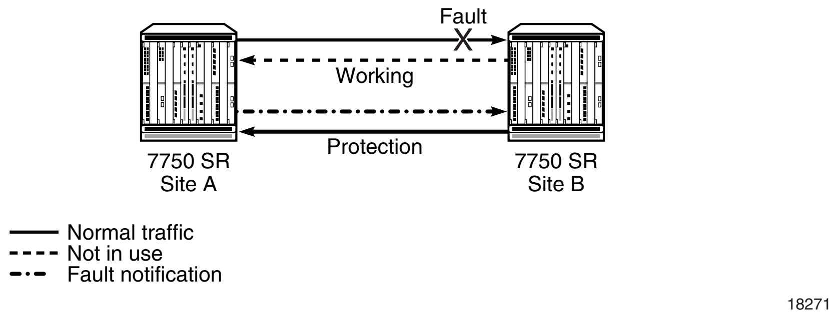
The working line degrades in the direction from site A to site B. Site B detects the fault and notifies site A of the fault using the protection line. Figure 40-2 shows the fault on the working line and site B notifying site A of the fault.

Figure 40-2 Site B detects the fault and notifies site A



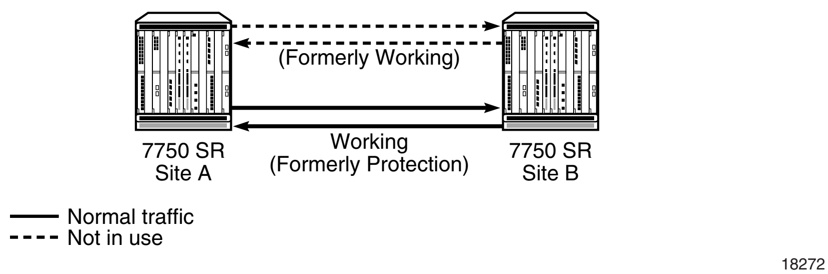
Site B automatically switches to the protection line. Site A receives the fault notification from site B and detects the fault on the working line. Site A acknowledges the fault and notifies site B that it is switching to the protection line. Figure 40-3 shows site B switching to the protection line and site A acknowledging the fault.

Figure 40-3 Site B switches to the protection line and site A acknowledges the fault



Site B receives the notification from site A and site A automatically switches to the protection line. Figure 40-4 shows normal operations resuming on the protection line between site A and site B. The protection line becomes and remains the working line since 1+1 APS is configured for non-revertive switching in this example.

Figure 40-4 Normal operations resume on the protection line



Configuring SAPs on APS-protected ports

You can use APS-protected ports to create SAPs for 5620 SAM services. The SAP list of a service creation form displays the APS-group SONET channels with all other SONET channels, but uses a different port ID format. An example of an APS group port ID is Channel aps-1.sts3-1. To create a SAP that uses an APS group, you must first configure the SONET channels in the APS group.

40.2 Workflow to manage APS

1 Create a 1+1 APS configuration on SONET/SDH ports:

i As required, create an SC APS group or MC APS group using SONET/SDH ports. Configure the operational state for each APS channel. See Procedures 40-1 and 40-2 for more information.

ii As required, create an SC APS IMA or MLPPP bundle or MC APS MLPPP bundle. See Procedures 40-3 and 40-4 for more information.

2 As required, change the operational state of an APS channel. See Procedure 40-5 for more information.

40.3 APS management procedures

Use the following procedures to perform APS management tasks.

Procedure 40-1 To create an SC APS group using SONET/SDH ports

Note — When a multiservice site is configured on an IOM, the working and protection ports must be configured on the same IOM.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure APS and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Groups object and choose Create APS Group from the contextual menu. The SC APS Group (Create) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the APS Group tab button.

7 Configure the parameters:

- Auto-Assign ID
- Group Number
- APS Mode
- Direction
- Revert Mode
- Wait To Restore (seconds)
- Annex B Command Switch

8 Click on the States tab button.

9 Configure the Administrative State parameter.

Note — When a working channel or protection channel is added to an APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

10 Click on the Apply button. An SC APS Group icon appears under the APS Groups object in the navigation tree.

11 Click on the APS Group tab button.

12 Configure the parameters:

- APS Mode
- Direction
- Revert Mode
- Wait To Restore (seconds)
- Annex B Command Switch
- Hold Time for Line Signal Degradation (100s of milliseconds)
- Hold Time for Line Signal Failure (100s of milliseconds)
- RDI Alarm Generation

13 Perform the following steps to configure the working and protection channels.

i Click on the APS Channels tab button.

ii Click on the Create button. The APS Channel (Create) form opens.

iii Configure the Channel Role parameter.

Note — If you are creating a 1+1 SC APS group, you must create the working channel before you create the protection channel.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button. A list of available ports is displayed.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the SC APS Group (Edit) form.

ix Click on the Create button. The APS Channel (Create) form opens.

x Repeat steps iii to viii to add the protection channel or second working channel.

xi Click on the Apply button.

14 Configure the operational state of the working and protection channels. Perform the following steps:

i Choose a channel from the list and click on the Properties button. The APS Channel - *Type* (Edit) form opens with the APS Channel tab displayed.

ii Configure the Command Switch parameter.

iii Click on the OK button. The APS Channel - *Type* (Edit) form closes.

15 Configure the APS common configuration parameters for the working and protection channels. Perform the following steps:

i Right-click on the SC APS Group icon in the navigation tree and choose Create APS SONET Channel from the contextual menu. The Sts*n* SONET Channel (Create) form opens with the General tab displayed.

ii Configure the channel as described in chapter 20.

iii Create all channels as described in chapter 20.

Procedure 40-2 To create an MC APS group using SONET/SDH ports

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Group (APS) from the object drop-down list.

3 Click on the Create button. The MC APS Group (Create) form opens.

4 Configure the Group Number parameter.

5 Click on the Select button to configure the Site Id parameter in the First Element panel. The Select a Network Element list form opens.

6 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the first NE in the MC APS group.

7 Click on the Select button to configure the Network Interface parameter in the First Element panel, if required. The Select a Network Element list form opens.

Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

8 Click on the Select button to configure the Site Id parameter in the Second Element panel. The Select a Network Element list form opens.

9 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the second NE in the MC APS group.

10 Click on the Select button to configure the Network Interface parameter in the Second Element panel, if required. The Select a Network Element list form opens.

Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

11 Click on the Apply button. An MC APS Group Member icon appears under the APS Groups object in the navigation tree of the selected First Element and Second Element NEs.

12 Click on the Members tab button to configure each MC APS group member.

13 Select a group member in the list and click on the Properties button. The MC APS Group Member (Edit) form opens with the General tab displayed.

14 Configure the Description parameter.

15 Click on the APS Group tab button.

16 Configure the parameters:

- Revert Mode
- Wait To Restore (seconds)

Note — The Wait To Restore (seconds) parameter is configurable when the Revert Mode parameter is set to revertive.

17 Click on the States tab button.

18 Configure the Administrative State parameter.

Note — When a working channel or protection channel is added to the APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

19 Click on the Multi Chassis tab button.

20 Configure the parameters:

- Advertise Interval (100s of milliseconds)
- Hold Time (100s of milliseconds)

21 Perform the following steps to configure an APS channel on the NE.

i Click on the APS Channels tab button.

ii Click on the Create button. The APS Channel (Create) form opens.

iii Configure the Channel Role parameter. If you have already created a working channel on the other MC APS group member, set this parameter to Protection. Otherwise, set this parameter to Working.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the form.

ix Click on the Apply button.

x Select the channel and click on the Properties button. The APS Channel - *Role* (Edit) form opens with the APS Channel tab displayed.

xi Configure the Command Switch parameter.

xii Click on the OK button. The APS Channel - *Role* (Edit) form closes.

xiii Click on the OK button. A dialog box appears.

xiv Click on the Yes button. The MC APS Group Member (Edit) form closes.

22 Repeat steps 13 to 21 to configure an APS channel on the other NE in the MC APS group.

23 Click on the OK button. The MC APS Group (Edit) form closes.

24 Close the Manage Node Redundancy form.

25 Perform the following steps to configure the MC APS parameters that are common to the working and protection channels.

i Right-click on the MC APS Group Member icon in the navigation tree and choose Create APS SONET Channel from the right-click contextual menu. The Sts*n* SONET Channel (Create) form opens with the General tab displayed.

ii Configure the SONET or SDH channels, as described in chapter 20.

Procedure 40-3 To create an SC APS IMA or MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on one NE. Consider the following when you add a DS0 channel that is a member of an APS group to an APS bundle:

- An APS channel can be a member of an APS bundle only, not of an IMA or multilink PPP bundle.
- All members of a working bundle must belong to a working channel of the same APS group.
- All members of a protection bundle must belong to a protection channel of the same APS group.

- You must create the working bundle before you can add an APS member to the APS bundle. If the member has a protection port, you must create the protection bundle before you can add the member to the APS bundle.
- You cannot delete the working port member of an APS bundle until you remove the member from the APS bundle.

The rules for adding a member to a bundle that is part of an APS bundle also apply to adding a member to a non-APS protected multilink bundle. See Procedures 19-28 and 19-30 for more information.

The following restrictions apply when adding a DS0 channel to an IMA bundle:

- The Clock Source parameter must be set to Node Timed.
- The encapsulation type of the DS0 channel must be ATM.

The following restrictions apply when adding a DS0 channel to a PPP bundle:

- All time slots on the DS0 channel must be selected.
- The encapsulation type of the DS0 channel must be IPCP.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure APS bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Bundles object and choose Create Bundle from the contextual menu. The APS Bundle Display form opens.

5 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

6 Click on the Next button.

7 Configure the parameters:

- Bundle Type

a If you set the Bundle Type parameter to IMA Group, configure the following parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

b If you set the Bundle Type parameter to PPP, configure the following parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

8 Click on the Finish button.

9 Click on the Close button. The APS Bundle Display form closes.

10 If the Bundle Type parameter is set to PPP in step 7, perform the following steps to configure the MLPPP bundle for multiclass service transmission.

Note — Consider the following when you configure MC MLPPP.

- MC MLPPP is supported only on channelized ASAP MDAs in a 7750 SR or 7710 SR.
- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab button.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number
- Stateless Aps Switchover

iv Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose a QoS profile, if required. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.

Note — You can only apply QoS profiles to an MC MLPPP bundle when the Class Count parameter is set to 4.

v Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

11 Click on the States tab button.

12 Configure the Administrative State parameter.

Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The APS Bundles (Edit) form closes.

15 To configure the APS working and protection bundles, perform the following steps.

Note — You must create the working bundle before you create the protection bundle.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Working Bundle from the contextual menu. The Create APS Working/Protecting Bundle form opens.

ii Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Daughter Card CLI Name
- Administrative State

iii Click on the Next button to view the configured bundle parameters.

iv Click on the Finish button.

v Click on the Close button. The Create APS Working/Protecting Bundle form closes.

vi Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Protection Bundle from the contextual menu. The Create Working/Protecting Bundle form opens.

vii Repeat steps ii to v to create the APS protection bundle.

16 To configure the administrative state of the APS working and protection bundles, perform the following steps.

Note — You must configure the End Point ID parameter on the APS PPP group before you change the working or protection bundle state.

i Right-click on the working bundle object below the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab button.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object below the SC APS Bundle object in the navigation tree. and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

17 To add members to the APS bundle, perform the following steps.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create Bundle Members from the contextual menu. The Add Bundle Member form opens.

ii Click on the Next button to add DS0 channel groups to the bundle. The Select Channels form opens.

iii Select a compatible channel from the list.

Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

iv Click on the Finish button and confirm the action. The Add Bundle Member form closes.

v Click on the Apply button.

vi Click on the Add button. The Add Bundle Member form opens.

vii Configure the Show Only Compatible Channels parameter.

viii Click on the Next button. The Select Channels form opens.

ix Select up to seven additional channels from the list.

x Click on the Finish button. A dialog box appears.

xi Click on the Yes button. The Add Bundle Members form closes.

xii Click on the Finish button.

xiii Click on the Close button. The Add Bundle Member form closes.

Procedure 40-4 To create an MC APS MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on two NEs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Bundles (Bundle) from the object drop-down list.

3 Click on the Create button. The MC APS Bundles (Create) form opens.

4 Configure the Bundle Number parameter.

5 Click on the Select button beside the First Network Element parameter. The Select a Network Element list form opens.

6 Select an NE in the list and click on the OK button. The Select a Network Element list form closes.

7 Click on the Select button beside the Second Network Element parameter. The Select a Network Element list form opens.

8 Select an NE in the list and click on the OK button. The Select a Network Element form closes.

9 Click on the OK button. An MC APS Bundle object appears in the navigation tree under the APS Bundles object of each specified NE.

10 Close the Manage Node Redundancy form.

11 Configure the MLPPP bundle for multiclass service transmission. Perform the following steps.

Note — Consider the following when you configure MC MLPPP.

- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the new MC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab button.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number
- Stateless Aps Switchover

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button.

12 Click on the States tab button.

13 Configure the Administrative State parameter.

Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The APS Bundles (Edit) form closes.

16 Perform the following steps to configure the MC APS working and protection bundles.

i Right-click on the MC APS Bundle object created in step 6 in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Protection and Working Bundles tab button.

iii Click on the Create button. The Create APS Working/Protecting Bundle form opens.

iv Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

v Click on the Select button beside the Daughter Card CLI Name parameter. The Select Daughter Card - Multilink Bundle list form opens.

vi Select a daughter card in the list and click on the OK button. The Select Daughter Card - Multilink Bundle list form closes.

vii Click on the Next button.

viii Configure the parameters.

- Bundle Type
- Protection Type

  The working bundle must be on the same NE as the APS working channel and the protection bundle must but on the same NE as the APS protection channel.

ix Click on the Finish button.

x Click on the Close button. The Create APS Working/Protecting Bundle form closes.

xi Close the APS Bundles (Edit) form.

xii Repeat steps i to xi to configure the MC APS protection bundle created in step 8.

17 Perform the following steps to configure the administrative state of the MC APS working and protection bundles.

i Right-click on the working bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab button.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

18 To add multilink bundle members, perform the following steps.

i Right-click on the MC APS Bundle object on either NE in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Bundle Members tab button.

iii Click on the Add button. The Add Bundle Member form opens.

iv Configure the Show Only Compatible Channels parameter.

v Click on the Next button. The Select Channels form opens.

vi Select a channel in the list.

Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

vii Click on the Finish button. A dialog box appears.

viii Click on the Yes button. The Add Bundle Members form closes.

ix Click on the Apply button.

x Click on the Add button. The Add Bundle Member form opens.

xi Configure the Show Only Compatible Channels parameter.

xii Click on the Next button. The Select Channels form opens.

xiii Select up to seven additional channels from the list.

xiv Click on the Finish button A dialog box appears.

xv Click on the Yes button. The Add Bundle Members form closes.

xvi Click on the OK button. The APS Bundles (Edit) form closes.

Procedure 40-5 To change the operational state of an SC APS channel

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to modify the APS channel and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon fully.

4 Right-click on the APS Channel object. The APS Channel (Edit) form opens.

5 Configure the Command Switch parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The operational state of the APS channel changes and the APS Channel (Edit) form closes.

Procedure 40-6 To delete an SC APS group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to delete an APS group and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Group object and choose Delete from the contextual menu. A dialog box appears.

Caution — Removing an APS group removes the working and protection channels and associated ports from the APS group, and deletes the APS group ID. Ensure that you select the correct APS group.

5 Click on the View Dependencies button. A dialog box appears.

6 Click on the OK button.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the SC APS group.

Procedure 40-7 To delete an SC APS bundle

Perform this procedure to permanently remove an SC APS bundle from the 5620 SAM and NE configurations.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to delete an APS bundle and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Right-click on the APS Bundle object and choose Delete from the contextual menu. A dialog box appears.

5 Click on the View Dependencies button. A dialog box appears.

6 Click on the OK button to proceed.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the SC APS bundle.

Procedure 40-8 To delete an MC APS group or bundle

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Perform one of the following.

   a Choose MC APS Group (APS) from the object drop-down list.

   b Choose MC APS Bundles (APS) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC APS groups or MC APS bundles appears.

4 Select an entry in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Select the I understand the implications of this action check box.

9 Click on the Yes button. The 5620 SAM deletes the MC APS group or bundle and the corresponding configuration on each member site.

41 — MC peer groups

41.1 MC peer groups overview

An MC peer group is a 5620 SAM object that defines the relationship between two peer NEs to provide system redundancy in an Ethernet network. An MC peer group configuration includes a list of protocols and objects with state information that is to be synchronized between the peers.

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR each support the creation of up to 20 MC peer groups using Ethernet ports in access mode. An MC peer group can contain one or more of the following child group objects:

- MC endpoint group—see chapter 42
- MC LAG group—see chapter 43
- MC synchronization group—see chapter 44
- MC ring group—see chapter 45

Note — Only the 7450 ESS, 7710 SR, and 7750 SR support the creation of MC endpoint groups.

When you create a child group object, the 5620 SAM automatically creates the child group members using the peer objects in the MC peer group.

The 5620 SAM automatically discovers MC peers that are configured on managed NEs and creates an MC peer group if the source address of each peer matches the peer address of the other. If an MC peer address on an NE is changed after discovery, for example, using a CLI, the 5620 SAM deletes the MC peer group but does not delete the peer configuration on either NE. When the mismatch is corrected, the 5620 SAM recreates the MC peer group.

When the MC peer addresses match but the 5620 SAM detects another MC peer group configuration mismatch, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form. The alarm information includes the type of configuration mismatch. When the mismatch is corrected, the alarm and check mark clear.

41.2 Workflow to manage MC peer groups

1. Create an MC peer group. See Procedure 41-1 for more information.
2. As required, configure an MC peer within an MC peer group. See Procedure 41-2 for more information.
3. As required, perform an on-demand protocol synchronization between MC peer group members. See Procedure 41-3 for more information.

41.3 MC peer groups management procedures

Use the following procedures to perform MC peer group management tasks.

Procedure 41-1 To configure an MC peer group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Perform one of the following:

   a Configure an existing MC peer group. Perform the following:

      i Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

      ii Select an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

      iii Go to step 4.

   b Create an MC peer group by performing the following:

Note — At least one MC peer must be a 5620 SAM-managed NE. The 5620 SAM raises an alarm when an MC peer group contains an unmanaged NE.

      i Click on the Create button. The MC Peer Group (Create) form opens with the General tab displayed.

      ii Click on the Select button in the First Element panel to choose the first site for the peer group. The Select Site Info form opens.

      iii Select an NE in the list and click on the OK button. The Select Site Info form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

      iv To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a virtual router interface form opens.

Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

      v Select an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

      vi Click on the Select button in the Second Element panel to choose the second site for the peer group. The Select Site Info form opens.

vii Select an NE in the list and click on the OK button. The Select Site Info form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

viii To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a virtual router interface form opens.

Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

ix Select an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

4 Configure the following parameters in the First Element panel:

- Source Address
- Peer Name
  If Peer Name parameter is not configured, the peer IP address is used by the MC endpoint.
- Description
- Authentication Key
- Administrative State

5 Configure the following parameters in the Second Element panel:

- Source Address
- Peer Name
  If Peer Name parameter is not configured, the peer IP address is used by the MC endpoint.
- Description
- Authentication Key
- Administrative State

6 Click on the Peer Synchronization tab button.

7 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber IPoE Management
- Subscriber PPPoE Management
- SRRP
- MC Ring
- MLD Snooping
- MC Ring

8 Click on the Apply button.

9 Click on the Associated Groups tab button.

10 Create an MC LAG, if required.

i Right-click on the MC LAG object in the components tree and choose Create MC LAG from the contextual menu. The MC LAG (Create) form opens.

ii Perform steps 7 to 11 in Procedure 43-1.

11 Create an MC synchronization group, if required.

i Right-click on the MC Sync Group object in the components tree and choose Create MC Sync Group from the contextual menu. The MC Sync Group (Create) form opens.

ii Perform steps 6 to 12 in Procedure 44-1.

12 Create an MC Ring Group, if required.

i Right-click on the MC Ring Group object in the components tree and choose Create MC Ring Group from the contextual menu. The MC Ring Group (Create) form opens.

ii Configure the Name parameter.

iii Click on the Select button beside the Synchronization Tag parameter. The Select Multi-Chassis Sync Group form opens.

iv Choose an MC synchronization group from the list and click on the OK button. The Select Multi-Chassis Sync Group form closes and the MC synchronization group is displayed on the MC Ring Group (Create) form.

13 Create an MC endpoint group, if required.

i Right-click on the MC Endpoint Group object in the components tree and choose Create Endpoint Group from the contextual menu. The MC Endpoint Group (Create) form opens.

ii Perform steps 2 to 5 in Procedure 42-1.

14 Click on the OK button. The MC Peer Group (Create) form closes.

15 Close the Manage Node Redundancy form.

Procedure 41-2 To configure an MC peer

Perform this procedure to modify an existing MC peer when there is a configuration mismatch with the other peer in an MC peer group.

Note — The MC peer parameters are configurable only when there is a configuration mismatch, which is indicated when the Neighbor Match check box on the MC Peer (Edit) form is unselected.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Select an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

5 Click on the Members tab button.

6 Select an entry in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Source Address
- Authentication Key
- Administrative State

8 Perform the following to configure the MC LAG group parameters.

i Click on the MC LAG tab button.

ii Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

9 Perform the following to configure the MC synchronization group parameters.

i Click on the Synchronization Protocol tab button.

ii Select an entry in the list and click on the Properties button. The MC Peer Sync (Edit) form opens.

iii Configure the parameters:

- Synchronize IGMP
- Synchronize IGMP-Snooping
- Synchronize Subscriber Management
- Synchronize SRRP
- Synchronize MC Ring
- Synchronize MLD Snooping
- Synchronize Subscriber Host Tracking

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MC Peer Sync (Edit) form closes.

12 Close the MC Peer (Edit) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 41-3 To perform an on-demand protocol synchronization between MC peer group members

Perform this procedure to distribute the most recent protocol synchronization configuration to each member of an MC peer group. This is required when the configurations do not match, for example, after the configuration is changed locally on only one MC peer using a CLI. When the peer configurations do not match, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Peer Synchronization tab button.

5 Click on the Resync button. The member configurations are synchronized.

6 Close the MC Synchronization (Edit) form.

7 Close the Manage Node Redundancy form.

Procedure 41-4 To delete an MC peer group

Caution — Deleting an MC peer group removes all of the MC configurations that are associated with the MC peer group, such as the following:

- MC LAG groups
- MC synchronization groups
- MC ring groups

Ensure that you specify the correct MC peer group for deletion in this procedure.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Select one or more MC peer groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A Warning form opens.

6 View the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC peer group and the corresponding configuration on each member site.

9 Close the Manage Node Redundancy form.

42 — MC endpoint groups

42.1 MC endpoint groups overview

An MC endpoint group consists of two MC endpoint peers that are configured as peers in a pair of sites. Multiple VPLS endpoints can use the MC endpoint peer. The endpoints must be on a 7450 ESS, 7710 SR, or 7750 SR, and must support PW redundancy. Each endpoint can be associated with different destinations, with a maximum of two spoke SDPs for each endpoint. The endpoints communicate with each other to get the associated status of the spoke SDPs, which ensures that only one spoke SDP is active at any time; the other spoke SDPs have a standby status. The grouping of multiple spoke SDPs that are associated with the two MC endpoint peers eliminates traffic loops in a VPLS or B-VPLS.

An MC endpoint group includes:

- two MC endpoint peers that can be used by a spoke SDP, which is under mc-endpoint and relies on mc-ep-peer in the CLI
- an MC protocol that is used for:
    - determination of which MC endpoint peers are active or standby
    - synchronization of the pseudo-wire information that is between the MC endpoint peers
    - fault detection using centralized BFD. The MC endpoint protocol contains a keep-alive mechanism because BFD cannot detect whether an MC endpoint peer is shut down or if there is a configuration problem.
- T-LDP signaling, which is used to communicate whether the pseudo-wire is active or standby to other gateway pairs. The other gateway pairs may not have an MC endpoint.

An MC peer group that is managed by the 5620 SAM contains two MC peers. Each MC peer is configured as the peer of the other MC peer. An MC peer group must be created before you create MC endpoint group. See chapter 41 for more information about MC peer groups.

BFD

The MC endpoint protocol uses the keep-alive mechanisms. The MC endpoint protocol also supports BFD to eliminate traffic loops. See Procedure 42-1 for information about how to configure an MC endpoint group for BFD.

42.2 Workflow to manage MC endpoint groups

1. Create an MC peer group, as described in chapter 41.
2. Create an MC endpoint group. See Procedure 42-1 for more information.
3. Create and configure the VPLS. See chapter 71 for more information.
4. As required, create an MC LAG group. See chapter 43 for more information.
5. As required, create an MC synchronization group. See chapter 44 for more information.
6. As required, create an MC ring group. See chapter 45 for more information.

42.3 MC endpoint groups management procedures

Use the following procedures to perform MC endpoint group management tasks.

Procedure 42-1 To configure an MC endpoint group

1 Create an MC peer group, as described in steps 1 to 13 of Procedure 41-1.

2 Configure the Description parameter.

3 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

4 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

5 Click on the OK button.

6 Create a VPLS, site, and VPLS endpoint, as described in steps 1 to 21 of Procedure 71-1.

Note — In step 21iii of Procedure 71-1, set the Endpoint Type parameter to Multi Chassis and perform steps 21iv to 21x.

7 Click on the Yes button.

8 Perform one of the following:

a Create a redundant spoke SDP binding under an endpoint, as described in steps 4 to 43 of Procedure 71-5.

b Create a spoke SDP binding for the site, as described in steps 9 to 43 of Procedure 71-5.

Procedure 42-2 To modify an MC endpoint group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the Select Object Type drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose an MC endpoint group and click on the Properties button. The MC Endpoint Group (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

7 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MC Endpoint Group form closes.

Procedure 42-3 To delete an MC endpoint group

Caution — When you perform this procedure, the MC endpoint group is deleted from the 5620 SAM and member NE configurations. In addition, deleting an MC endpoint group removes all of the MC configurations that are associated with the MC peer group.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the object list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose one or more MC endpoint groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A warning form opens.

6 View the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC endpoint group and the corresponding configuration for each member site.

If there are MC endpoints that use the MC endpoint group, you cannot delete the MC endpoint group. Remove the MC endpoints from the MC endpoint group and repeat steps 1 to 9.

9 Close the Manage Node Redundancy form.

43 — MC LAG groups

43.1 MC LAG groups overview

A LAG is a group of physical ports that form one logical link between two NEs to increase bandwidth, allow load balancing, and provide seamless redundancy. LAG support over multiple devices provides node-level redundancy in addition to link-layer redundancy using a switchover function. An MC LAG configuration provides redundant L2 access connectivity that extends beyond link-layer protection by allowing two devices to share a common LAG end point.

An MC LAG configuration includes one active member NE and one standby member NE. The active and standby NEs synchronize the link state information to facilitate link-layer messaging between an access node and each NE. This active and standby NE coupling provides a synchronized forwarding plane to and from the access node. LACP is used to manage the active and standby states of the available LAG links; only the links of one member NE at a time are active.

The 7450 ESS, 7710 SR, and 7750 SR support the creation of MC LAG groups using Ethernet ports in Access mode.

Note — You can create an MC LAG group only from within an existing MC peer group. See chapter 41 for more information about MC peer groups.

When you use the 5620 SAM to change the MC LAG configuration on an NE, the 5620 SAM automatically updates the MC LAG configuration on the other NE. When you change the MC LAG configuration on an NE using, for example, a CLI, the 5620 SAM detects the configuration mismatch between the NEs and raises an alarm. The alarm information includes the type of configuration mismatch.

MC synchronization

When subscriber management is enabled on an NE in an MC LAG configuration, the NE maintains dynamic state information for each subscriber host. The active and standby NEs synchronize this information to ensure uninterrupted service delivery in the case of an MC LAG switchover.

See chapter 44 for more information about MC synchronization.

43.2 Workflow to manage MC LAG groups

1. Create one or more LAGs using Ethernet access ports, as required. See chapter 18 for more information.
2. Create an MC peer group. See chapter 41 for more information.
3. Create an MC LAG group. See Procedure 43-1 for more information.
4. As required, configure MC LAG group members. See Procedure 43-2 for more information.

43.3 MC LAG groups management procedures

Use the following procedures to perform MC LAG management tasks.

Procedure 43-1 To create an MC LAG group

Perform this procedure to create an MC LAG group or to modify an existing MC LAG group. Consider the following before you create an MC LAG group:

- You can create an MC LAG member only on an Ethernet MDA.
- MC LAG member ports must be in Access mode.
- The 5620 SAM assigns the same LACP key, system ID, and system priority to each MC LAG member.
- MC LAGs are not supported when MAC subnetting is enabled.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Click on the Search button. A list of MC peer groups is displayed.

4 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

5 Click on the Associated Groups tab button.

6 Right-click on the MC Lag object in the navigation tree and choose Create MC LAG Group. The MC LAG Group (Create) form opens.

7 Configure the parameters:

- LACP Key
- System ID
- System Priority
- Description

8 Configure the PBB Source Backbone MAC LSB parameters:

- Use LACP Key
- MAC LSB (hex)

Note 1 — The parameters are only configurable on the 7750 SR, 7750 SR-c12, and 7450 ESS. The NE must also be configured with an IOM 3 MDA.

Note 2 — An MC LAG has two members. The parameters can be configured only when both peers are PBB-capable; for example, if the peers are either the 7750 SR, 7750 SR-c12, or 7450 ESS. If both peers are PBB-incapable, the PBB parameters are not displayed.

9 Perform the following steps to choose the LAG for the first MC LAG member.

   i Click on the Select button beside the LAG ID parameter in the First Site panel. The Select LAG form opens.

   ii If no LAGs are listed, you can create a LAG by clicking on the Create button and performing steps 5 to 24 of Procedure 18-13.

   iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

10 Perform the following steps to choose the LAG for the first MC LAG member.

> **Note —** If you are configuring access dual-homing with local switching over PBB tunnels, the L2 access interfaces must be on LAGs that participate in the MC LAG. See Procedure 70-13 to configure L2 access interfaces.

   i Click on the Select button beside the LAG ID parameter in the Second Site panel. The Select LAG form opens.

   ii If no LAGs appear in the list, you can create a LAG by clicking on the Create button and performing steps 5 to 24 of Procedure 18-13.

   iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

11 Click on the OK button. The MC LAG (Create) form closes, and the new MC LAG object is displayed below the MC LAG object in the navigation tree on the MC Peer Group (Edit) form.

12 Close the MC Peer Group (Edit) form.

13 Close the Manage Node Redundancy form.

Procedure 43-2 To configure an MC LAG group member

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAGs is displayed.

4 Select an MC LAG in the list and click on the Properties button. The MC LAG Group (Edit) form opens with the General tab displayed.

5 Configure the MC LAG parameters that are common to each member, if required:

- LACP Key
- System ID
- System Priority
- Description

6 Click on the States tab button.

7 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the First Site panel. The MC Peer (Edit) form opens with the General tab displayed.

8 Configure the MC LAG member by performing the following steps.

i Click on the MC LAG tab button. The General tab is displayed.

ii Configure the parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The MC Peer (Edit) form closes.

9 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the Second Site panel. The NE Synchronization (Edit) form opens with the General tab displayed.

10 Repeat step 8.

11 Close the MC LAG Group (Edit) form.

12 Close the Manage Node Redundancy form.

Procedure 43-3 To delete an MC LAG group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAG groups is displayed.

4 Select one or more MC LAG groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. An information dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Click on the Yes button. The 5620 SAM deletes the MC LAG group and the corresponding configuration on each member site.

Note — If you change the default values of the Keep-Alive Interval (deciseconds) and Lost Connection Wait Interval parameters in step 8ii of Procedure 43-2, the MC LAG group configuration of the member sites is not removed. You can view the MC LAG member information under the LAG icon in the network view of the navigation tree.

9 Close the Manage Node Redundancy form.

44 — MC synchronization groups

44.1 MC synchronization groups overview

When subscriber management is enabled on an NE, the NE maintains dynamic subscriber-host state information. The state information must be synchronized between the active and standby NEs in a redundant configuration to ensure that service delivery is uninterrupted if a switchover occurs.

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR support the creation of MC synchronization groups using Ethernet ports in Access mode.

Note — You can create an MC synchronization group only from within an existing MC peer group. See chapter 41 for more information about MC peer groups.

MC synchronization can be used to ensure that the following dynamic state information is synchronized:

- Basic and enhanced subscriber management
- IGMP snooping in VPLS
- IGMP on IES or VPRN group interfaces
- SRRP in VPRN

You create an MC synchronization group inside an MC peer group using a unique synchronization tag to define the pair of NEs and the two ports or LAGs on which the dynamic state information is synchronized. The synchronization is applied to all SAPS on the port or LAG that have the same synchronization tag.

A synchronization tag can be applied to a specified VLAN range on a port or LAG. All of the SAPs in the VLAN range are assigned the synchronization tag. The SAPs that are not in the VLAN range are not synchronized.

Note 1 — Only ports and LAGs that use dot1q or Q in Q encapsulation support MC synchronization.

Note 2 — MC synchronization group VLAN ranges are configurable only after MC synchronization group creation.

Note 3 — If the 5620 SAM detects a port or VLAN range configuration mismatch in an MC synchronization group during NE discovery, the 5620 SAM raises an alarm.

MC synchronization and dual-homed L2/L3 CO

MC synchronization is typically used in a dual-homed L2 or L3 CO configuration. For example, an access node that aggregates several subscriber lines can be dual-homed to a redundant pair of NEs. Dynamic subscriber-host state information on the NE must be synchronized with the redundant peer to ensure that service delivery in unaffected if a switchover occurs. See chapters 73 and 74 for more information about L2 and L3 CO dual homing.

MC synchronization for dual homing requires the configuration of protocol synchronization on the MC peer group that defines the redundant pair of NEs. See Procedure 41-1 for more information about configuring protocol synchronization on an MC peer group.

44.2 Workflow to manage MC synchronization groups

1. Create an MC peer group. See chapter 41 for information about MC peer groups.
2. Create an MC synchronization group, including MC peer synchronization ports or VLAN ranges. See Procedure 44-1 for more information.
3. Configure protocol synchronization for the MC synchronization group. See Procedure 44-2 for more information.

44.3 MC synchronization groups managment procedures

Use the following procedures to perform MC synchronization management tasks.

Procedure 44-1 To create an MC synchronization group

1. Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.
2. Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.
3. Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.
4. Click on the Associated Groups tab button.
5. Right-click on the MC Sync Group object in the navigation tree and choose Create MC Sync Group from the drop-down menu. The MC Sync Group (Create) form opens.
6. Configure the parameters:
   - Synchronization Tag
   - Description
   - Sync Tag Config Level
7. Specify the port or LAG on the first NE.

   Click on the Select button beside the Port/LAG Name parameter in the First Element panel. The Select Port/LAG - MC Sync Group form opens.

   Note — If you set the Sync Tag Config Level parameter to VLAN Range Level, only dot1q and Q in Q-encapsulated Ethernet ports or LAGs in Access mode are listed.

8 Select a port or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

9 Specify the port or LAG on the second NE.

Click on the Select button beside the Port/LAG Name parameter in the Second Element panel. The Select Port/LAG - MC Sync Group form opens.

Note — Only ports or LAGs that have the same encapsulation type as the port or LAG on the first NE are listed.

10 Select a port or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

11 If you set the Sync Tag Config Level parameter to VLAN Range Level, perform the following steps to specify the VLAN ranges that the MC synchronization group is to monitor.

Note — The VLAN ranges that you configure are applied to the configuration of each site in the MC synchronization group.

i Click on the Apply button. The form displays additional tabs.

ii Click on the First Site VLAN Entries tab button.

iii Click on the Create button. The VLAN Range (Create) form opens.

iv Configure the parameters:

- Minimum Outer Encap Value
- Maximum Outer Encap Value
- Minimum Inner Encap Value
- Maximum Inner Encap Value

The Minimum Inner Encap Value and Maximum Inner Encap Value parameters are configurable only when the encapsulation type of the associated ports or LAGs is Q in Q.

v Click on the OK button. The VLAN Range (Create) form closes.

vi Repeat steps 11 iii to v to add another VLAN range, if required.

12 Close the MC Sync Group (Create) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 44-2 To configure protocol synchronization between MC peer group members

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Synchronize Protocols tab button.

5 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber Management
- SRRP
- MC Ring
- MLD Snooping
- MC Ring

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The MC Synchronization (Edit) form closes.

8 Close the Manage Node Redundancy form.

Procedure 44-3 To delete an MC synchronization group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Sync Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC synchronization groups is displayed.

4 Select one or more MC synchronization groups in the list and click on the Delete button. A dialog box appears.

Caution — Deleting an MC synchronization group that is associated with an MC ring group disables the protocol synchronization between the member sites in the MC ring group.

5 Click on the Yes button. The 5620 SAM deletes the MC synchronization group and the corresponding configuration on each member site.

6 Close the Manage Node Redundancy form.

45 — MC ring groups

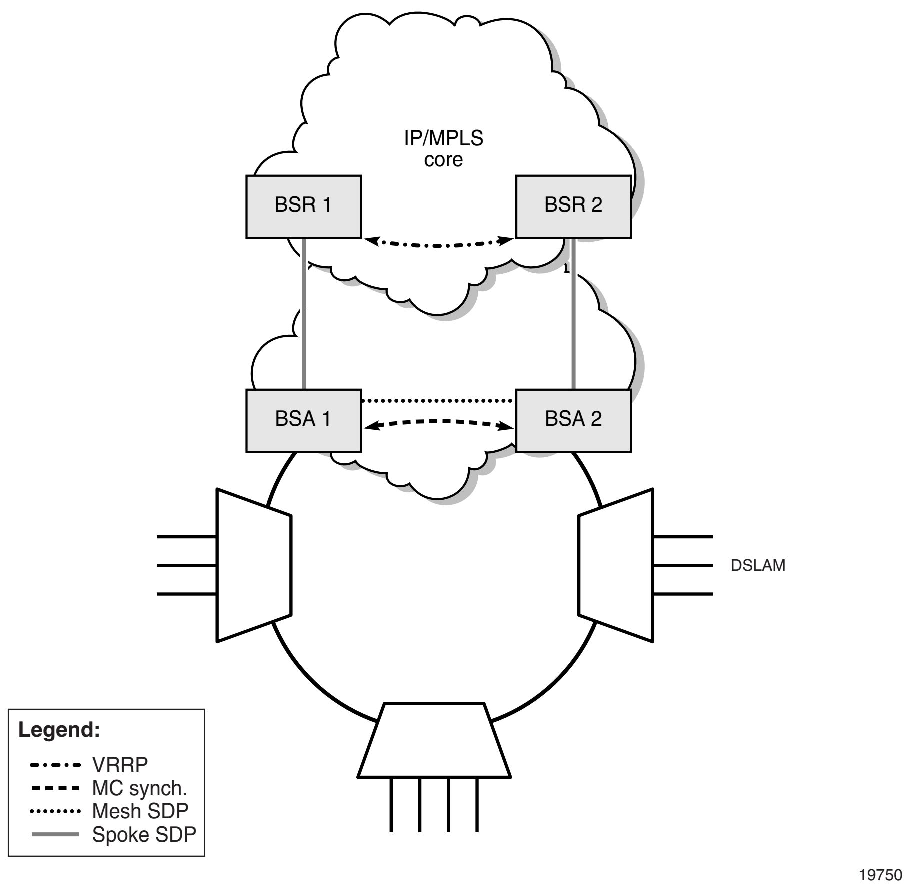
45.1 MC ring groups overview

5620 SAM MC ring groups are an extension of the dual-homing support available in TPSDA networks. MC ring groups provide aggregation redundancy in networks that have multiple access nodes, called ring nodes in the context of MC ring groups, connected in a single ring.

The 7210 SAS-M, 7450 ESS, 7710 SR, and 7750 SR support the creation of MC ring groups using Ethernet ports in Access mode.

Figure 45-1 shows a simple subscriber aggregation network in which a single ring of access nodes, such as DSLAMs, is connected to a BSA in a VPLS. Each BSA is connected to an IES or VPRN L3 interface on a BSR using a spoke SDP. Each BSR L3 interface aggregates the subscriber traffic in one subnet.

Figure 45-1 Simple subscriber aggregation network



Note 1 — BTV distribution is typically implemented in a separate VPLS that uses one SAP per access node.

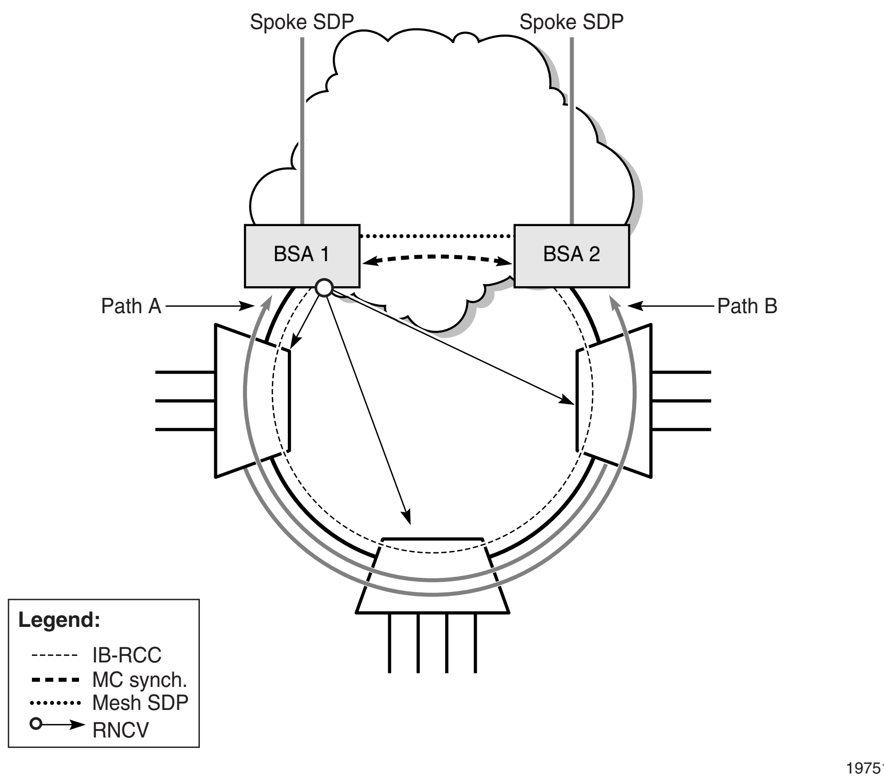
Note 2 — An MC ring group does not support a ring that has more than one break.

Steady-state condition

When an MC ring group is configured, the operation of a typical dual-homed ring is as shown in Figure 45-2. A steady-state condition is defined by the following.

- The participating BSAs have matching MC ring configurations.
- The In-Band Ring Control Connection, or IB-RCC, is operationally up.
- The MC ring is operationally up.

Figure 45-2 Dual-homed ring, steady-state condition



The IB-RCC is set up using a BFD session between IES or VPRN IP interfaces on BSA 1 and BSA 2. This connection requires a separate ring VLAN.

Note — You can create an MC ring group only from within an existing MC peer group. See chapter 41 for more information about MC peer groups.

In the steady state, the ring is fully closed and each ring node has two paths to the VPLS core; these are shown as Path A and Path B. To prevent a communication loop, a ring node can use only one path for VLAN traffic. The VLAN range can be explicitly assigned to Path B on each BSA; by default, the SAP uses Path A. The VLAN range assignment for each path must be the same on each BSA. A SAP in the conflict range is assigned to Path A, regardless of the local configuration.

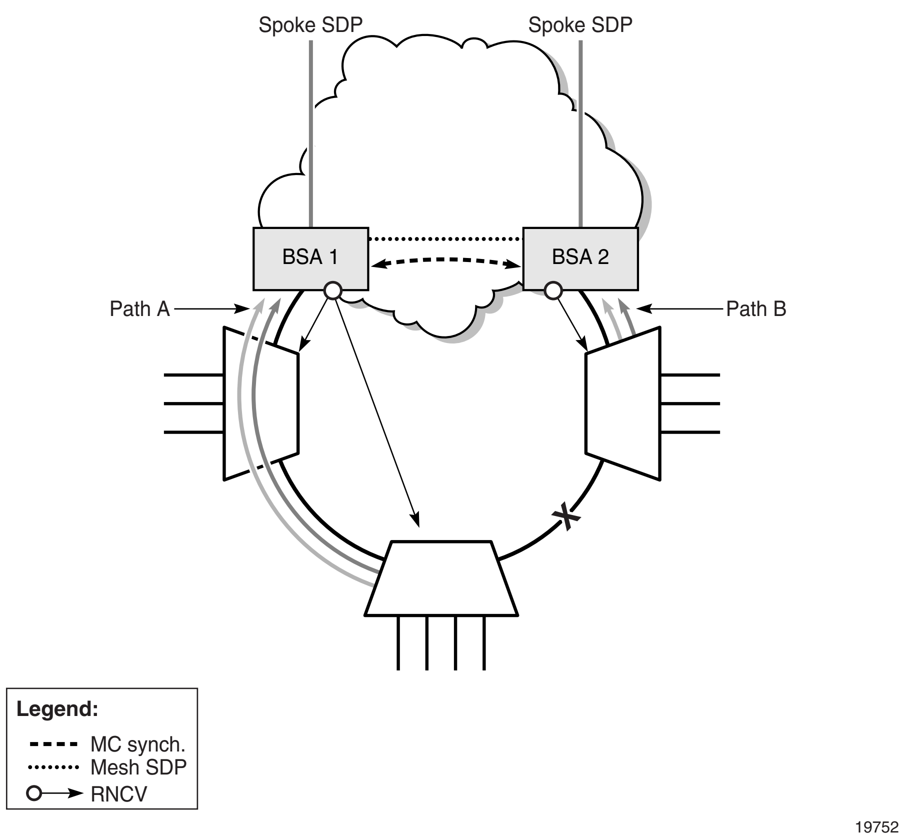
Each SAP in the path that ends on the master BSA is operationally up. Each subscriber-host forwarding database entry associated with the SAP points to the SAP. Each SAP in the path that ends on the standby BSA is operationally down. Each subscriber-host forwarding database entry associated with the SAP points to the mesh SDP that connects to the master BSA.

The master BSA periodically performs a Ring Node Connectivity Verification, or RNCV, check. The loss of connectivity to a ring node does not automatically trigger a switchover to the other path; if the IB-RCC BFD session is up, the ring is considered closed, and the master and standby BSA roles do not change.

Broken ring condition

A broken ring condition occurs when there is a link failure or ring node failure, as shown in Figure 45-3. In this condition, the IB-RCC is operationally down. Each ring node has only one path to the VPLS core.

Figure 45-3 Dual-homed ring, broken-ring condition



Each BSA becomes the master for the ring nodes that it can reach, and performs as described in the steady-state condition. Each L2 SAP on each BSA is operationally up, except the SAPs that are explicitly excluded from the MC ring control.

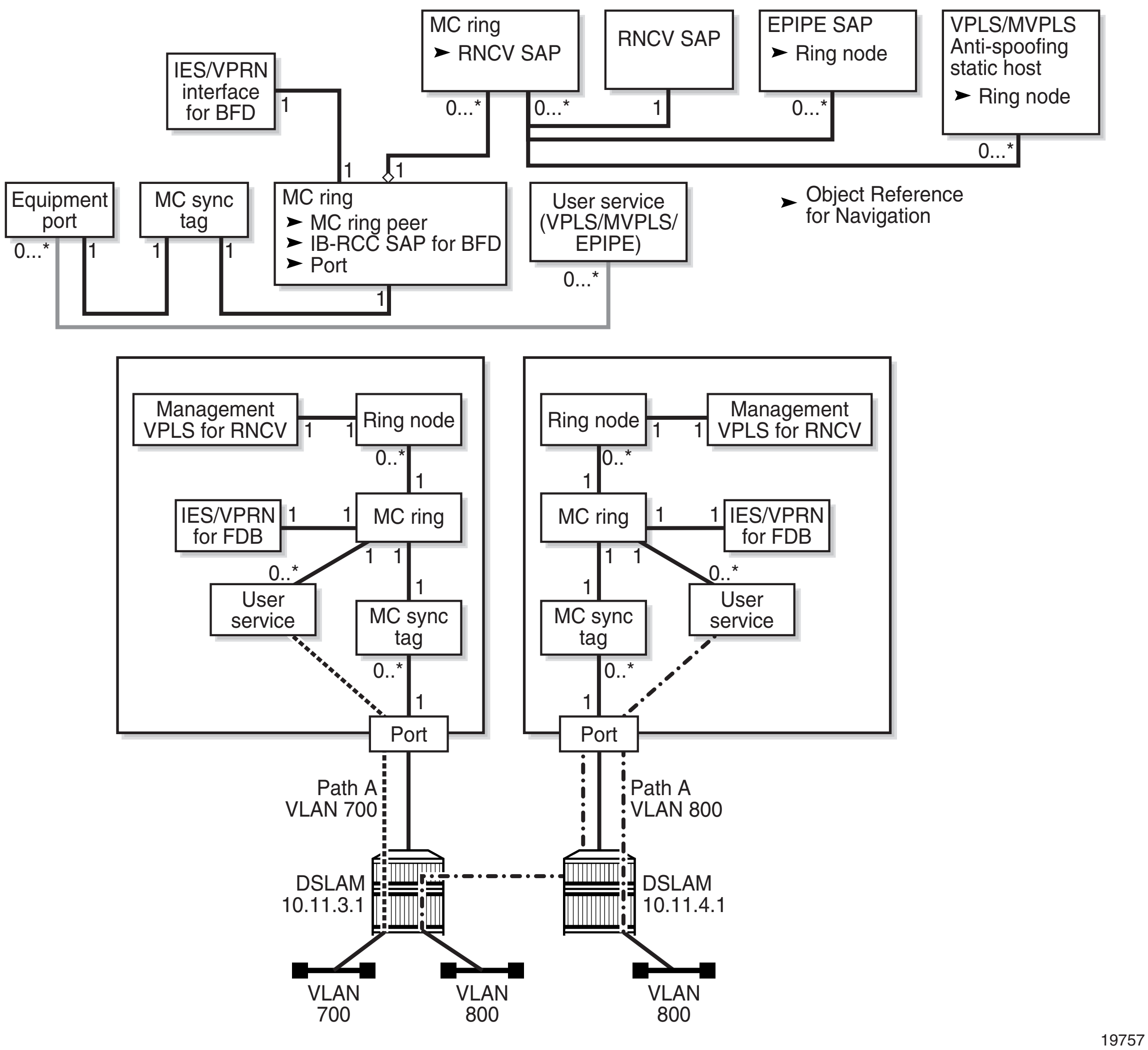
In the broken-ring condition, each BSA performs an RNCV check because each is a master. The forwarding database entry for each subscriber host behind a unreachable ring node points to the mesh SDP.

When the MC ring connectivity is restored, one BSA is the master for Path A and the other BSA is the master for Path B.

Object relationships

Figure 45-4 shows the MC ring and ring node object relationships with equipment and service objects.

Figure 45-4 MC ring group object relationships



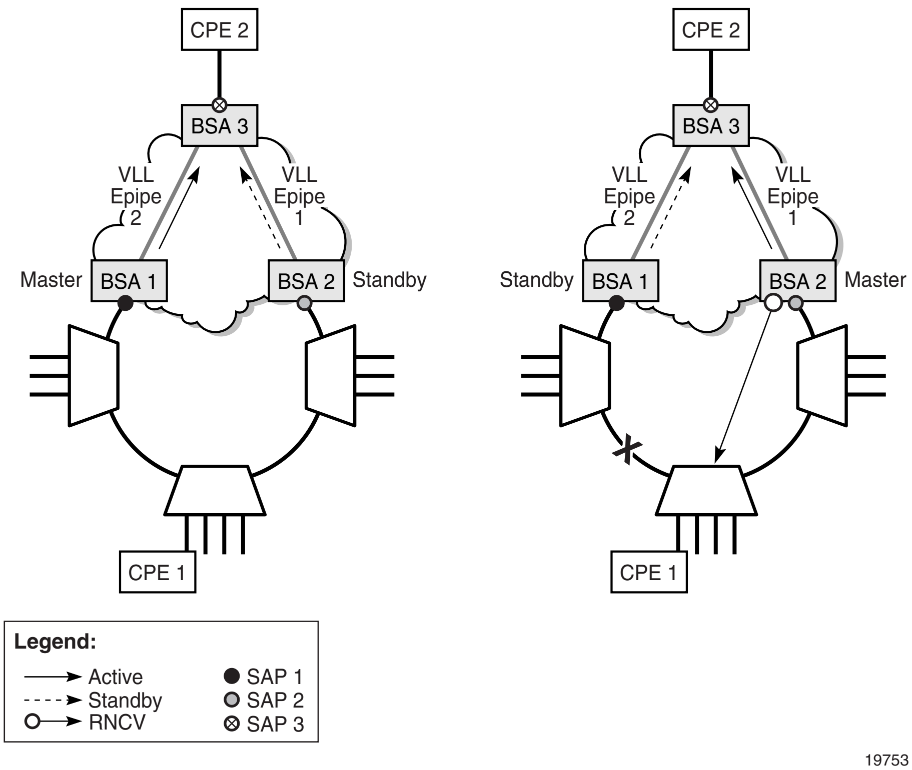
An MC ring has a one-to-one relationship with an MC synchronization tag. An MC ring uses one IES or VPRN service for IB-RCC. An MC ring can have multiple ring nodes, and each ring node can use only one SAP for RNCV.

When an MC ring group is correctly configured, each BSA L2 SAP is protected by the ring. The service that contains these protected SAPs is referred to as the user service. The service that is used for RNCV is an MVPLS that can also contain user SAPs and be a user service.

MC ring group and redundant VLL Epipe access operation

An MC ring group can connect to a VLL SAP to support redundant VLL Epipe access. Figure 45-5 shows a sample configuration using a VLL Epipe.

Figure 45-5 Dual-homed VLL Epipe configuration



CPE 1 connects to a ring node that has access to each BSA through a VLAN that is provisioned on each ring node. The SAP on each BSA uses the same VLAN tag.

In the closed ring on the left, BSA 1 is the master and sends an active status notification to BSA 3 on a VLL Epipe. BSA 2, the standby, sends a standby status notification. Based on this information, BSA 3 chooses a path to reach CPE 2.

In the broken ring on the right, the BSA that can use RNCV to reach CPE 1 becomes the master and sends an active status notification to BSA 3 on a VLL Epipe.

In each scenario, only one SAP is operationally up at a time, and each Epipe must be operationally up. If the ring node of CPE 1 is operationally down, neither BSA can reach the ring node, so each SAP and Epipe is operationally down.

MC ring groups and subscriber hosts

Each subscriber host on a SAP that is protected by an MC ring group must be associated with a ring node to determine whether the subscriber host is reachable by the BSA. Each VLL Epipe used for forwarding from an MC ring group must be explicitly configured with the name of a ring node in the MC ring. See Procedure 45-3 for information about configuring VLL Epipes for use with an MC ring group.

When subscriber management is enabled on a VPLS SAP, each dynamic subscriber host is automatically associated with a ring node. Static hosts on a VPLS SAP require explicit configuration. The following must be true before you can turn up an MC ring on a VPLS SAP that has one or more static hosts, or turn up a static host on a VPLS SAP in an operational MC ring:

- Subscriber management is enabled.
- The following are configured on the static host:
    - the name of a ring node in the MC ring group
    - subscriber identification
    - a subscriber profile
    - an SLA profile

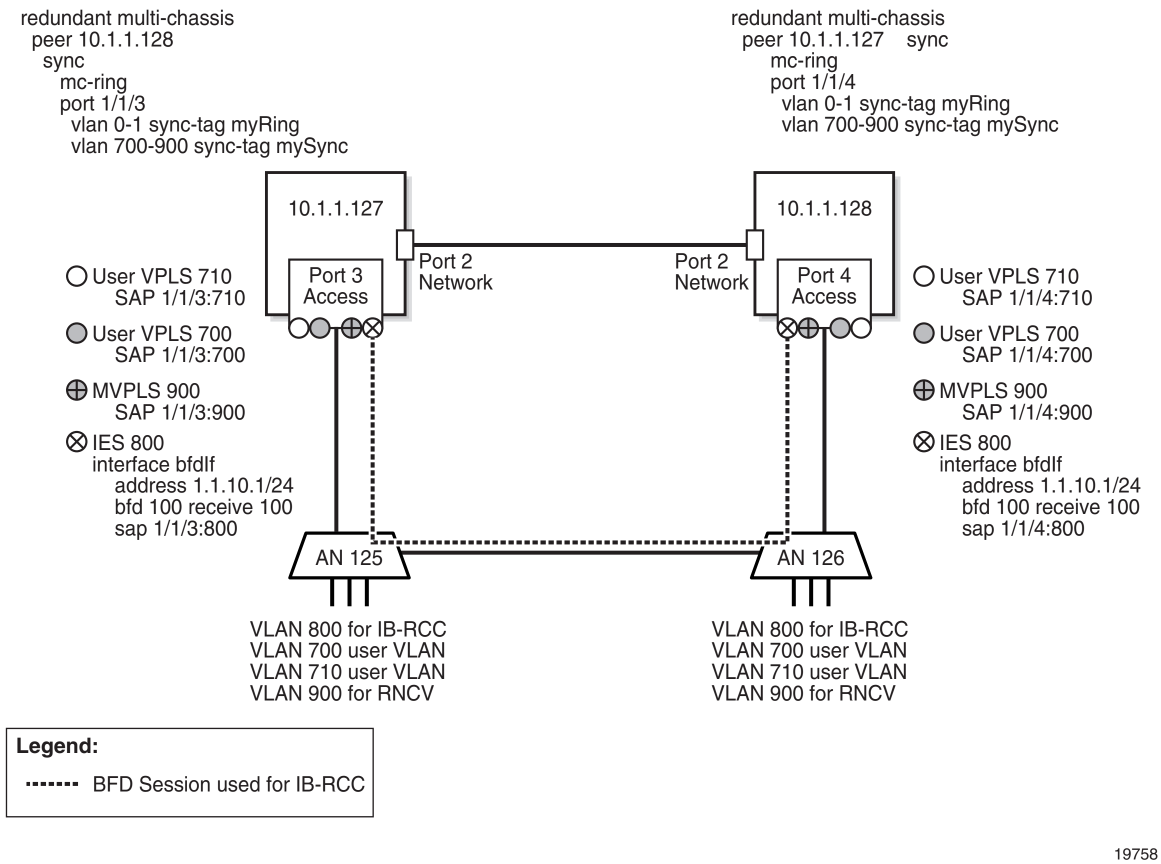
45.2 Workflow to manage MC ring groups

The following are the high-level steps required to perform MC ring group management.

NE preconfiguration

1 Configure physical connectivity between the two BSAs and the ring nodes, as shown in Figure 45-6. Each port must be operationally up.

Figure 45-6 MC ring group preconfiguration



2 Configure a routing protocol on each BSA to enable IP communication. See chapter 31 for information about configuring routing protocols.

3 Configure an MVPLS for RNCV on the BSAs. See chapter 71 for information about configuring MVPLS.

4 Create an MC peer group that has the two BSAs as members and has MC ring synchronization enabled. See chapter 41 for information about MC peer groups.

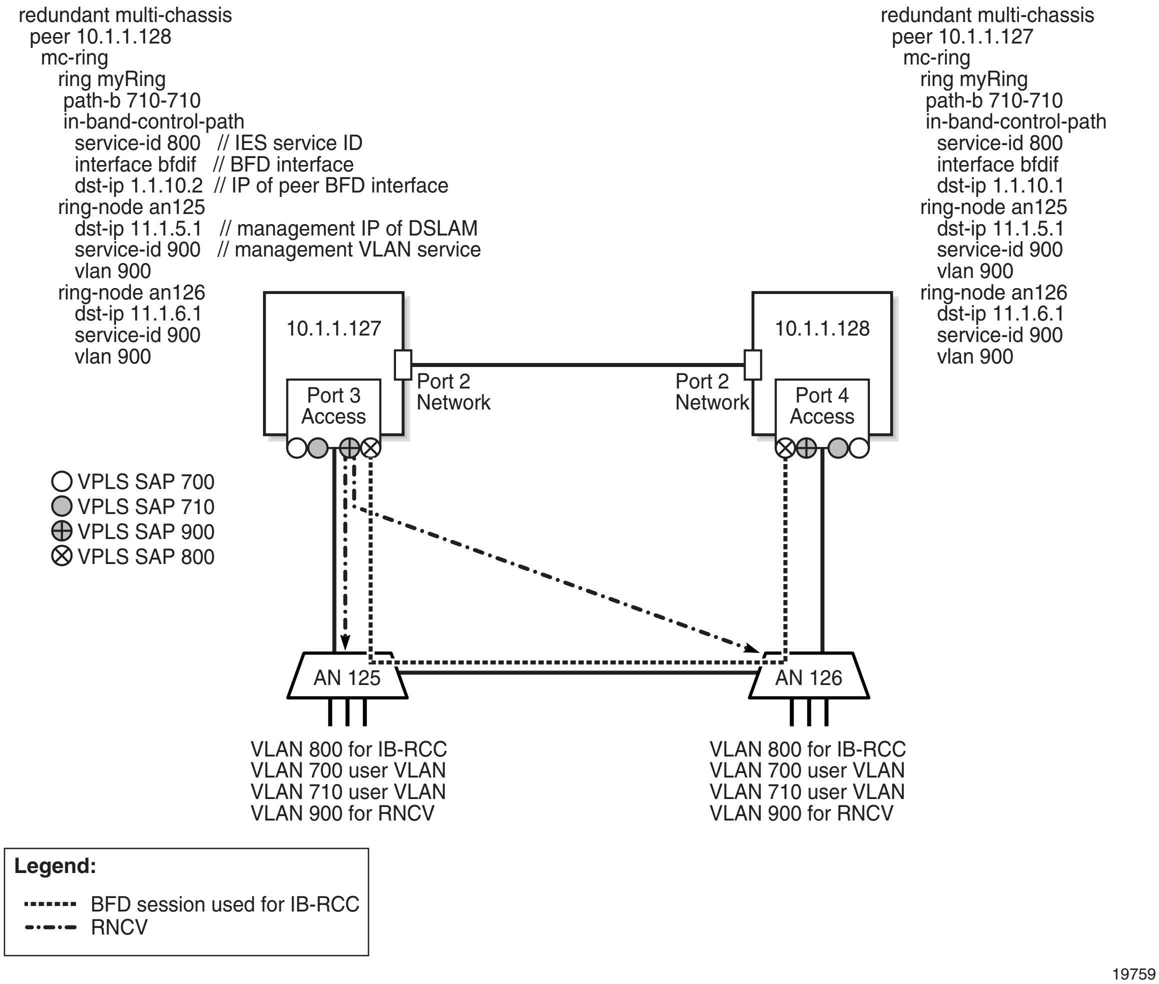
5 In the MC peer group, create an MC synchronization group that specifies each BSA access port. The MC synchronization group can synchronize the port or a VLAN range. See chapter 44 for information about MC synchronization groups.

6 Configure each ring node with the VLAN tag used for BFD to enable BFD communication through the ring. After this, each BSA SAP should be operational.

MC ring group configuration

7 Create an MC ring group that contains the BSAs (shown as 10.1.1.127 and 10.1.1.128 in Figure 45-7). For each ring node within the ring group, you must specify the management IP address of a ring node as the destination IP address and assign one VLAN for connectivity checking, shown in Figure 45-7 as VLAN 900. See Procedure 45-1 for more information.

Figure 45-7 MC ring configuration



8 Create the user VPLS and assign a SAP to each of the two BSA access ports. You can configure a protecting SAP on each BSA to provide SAP-level redundancy, if required. See chapter 71 for more information.

9 If the VPLS is to send traffic to an IES or a VPRN service, perform the following steps.

   i Create a spoke SDP from each VPLS site in the MC ring group to the IES or VPRN service.

   ii Configure traffic forwarding to the IES or VPRN service. See Procedure 45-2 for more information.

10 If the VPLS is to send traffic to redundant VLL Epipes, perform the following steps.

   i Create a redundant VLL Epipe from each VPLS site in the MC ring group to the BSA that is the common endpoint of the VLL Epipes.

   ii Configure traffic forwarding to each VLL Epipe service. See Procedure 45-3 for more information.

11 If the VPLS is to send traffic to an IES or a VPRN service, create a spoke SDP from the VPLS to the IES or VPRN service. See Procedure 45-2 for information about configuring the spoke SDP to send traffic from the MVPLS to an IES or a VPRN service.

12 Turn up the MC ring.

At this point, the following statements apply to the Figure 45-7 configuration.

- VPLS SAP 700 is operationally up on BSA 10.1.1.127 and operationally down on BSA 10.1.1.128.
- VPLS SAP 710 is operationally down on BSA 10.1.1.127 and operationally up on BSA 10.1.1.128.
- The operational state of the ring is Connected.

To test the configuration, you can shut down an access-node port in the ring to break the ring. As a result, the BSA SAPs should remain operationally up, but the operational state of the ring changes to Broken.

45.3 MC ring groups management procedures

Use the following procedures to perform MC ring group management tasks.

Procedure 45-1 To create an MC ring group

Note — You cannot create an MC ring SAP on a VPLS site that is the endpoint of redundant spoke SDPs.

1 Perform the NE preconfiguration steps in the workflow of this chapter.

2 Before you can deploy an MC ring to the participating BSAs, you must create an MC synchronization group. Perform Procedure 44-1 to create an MC synchronization group for the BSAs.

3 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

4 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of previously created MC peer groups is displayed. See chapter 41 for information about creating MC peer groups.

5 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

6 Click on the Associated Groups tab button.

7 Right-click on the MC Ring Group object and choose Create MC Ring Group from the drop-down menu. The MC Ring Group (Create) form opens.

8 Configure the parameters:

- Name
- Synchronization Tag

9 Click on the Apply button. The form displays additional tabs.

10 Click on the Properties button in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens with the General tab displayed.

11 Configure the parameters:

- Interface Name
- Service ID
- Destination IP Address

12 Perform the following steps to create a ring node.

i Click on the Components tab button.

ii Right-click on the MC Ring object and choose Create MC Ring Node. The MC Ring Node (Create) form opens.

iii Configure the parameters:

- Ring Node Name
- SAP Service ID
- SAP Outer Encapsulation Value
- SAP Inner Encapsulation Value
- Source IP Address
- Destination IP Address
- Source MAC Address
- Interval (minutes)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The MC Ring Node (Create) form closes.

vi Repeat steps 12 ii to v to create an additional ring node, if required.

13 To configure a VLAN range for traffic that is to use the non-default path through the MC ring, perform the following steps.

i Click on the Path B VLAN Range tab button.

ii Click on the Create button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

14 To configure a VLAN range for traffic that is not to be protected by the MC ring, perform the following steps.

- **i** Click on the Exclude VLAN Range tab button. The Exclude VLAN Range (Create) form opens.
- **ii** Click on the Create button. The Path B VLAN Range (Create) form opens.
- **iii** Configure the parameters:
  - Start VLAN Value
  - End VLAN Value
- **iv** Click on the OK button. A dialog box appears.
- **v** Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MC Ring (Edit) form closes.

17 Click on the Properties button in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens with the General tab displayed.

18 Repeat steps 11 to 16.

19 Close the MC Ring Group (Create) form.

Procedure 45-2 To configure L3 forwarding from a VPLS or MVPLS to an IES or VPRN service

Perform this procedure to configure MC ring group traffic forwarding through a BSA spoke SDP to a BSR L3 access interface in an IES or VPRN service, as shown in Figure 45-1. See chapter 71 for information about creating and configuring VPLS and MVPLS services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VPLS or MVPLS in the list and click on the Properties button. The service properties form opens.

4 On the navigation tree, click on a site. The site properties form opens.

5 Click on the Default Gateway tab button.

6 Configure the parameters, which specify the IP and MAC address of the default gateway to which the VPLS is to forward L3 traffic.

7 Click on the OK button. The site properties form closes.

8 Click on the OK button. The service properties form closes.

Procedure 45-3 To configure an MC ring group for redundant VLL Epipe access

Perform this procedure to configure traffic forwarding from a BSA SAP in an MC ring group through a VLL Epipe to a BSA SAP outside the ring group, as shown in Figure 45-5. See chapter 70 for information about creating and configuring VLL Epipe services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VLL Epipe service in the list and click on the Properties button. The Epipe Service (Edit) form opens.

4 On the navigation tree, right-click on an L2 access interface. The L2 Access Interface (Edit) form opens with the General tab displayed.

5 Perform one of the following to specify a ring node in the ring group that terminates on the port associated with the L2 access interface.

- **a** Perform the following steps to select the ring node from a list.
  - **i** Click on the Select button in the MC Redundancy panel. The Select form opens.
  - **ii** Select a ring node in the list and click on the OK button. The Select form closes, and the ring node name is displayed on the L2 Access Interface (Edit) form.
- **b** Type the name of the ring node in the MC Ring Node field.

6 Click on the OK button. The L2 Access Interface (Edit) form closes, and a dialog box appears.

7 Click on the OK button. The Epipe Service (Edit) form reappears.

8 Click on the OK button.A dialog box appears.

9 Click on the Yes button. The Epipe Service (Edit) form closes.

Procedure 45-4 To turn up the MC rings in an MC ring group

Note 1 — You cannot administratively enable an MC ring group in one operation; you must turn up the MC rings in the MC ring group individually.

Note 2 — If a Problems Encountered form is displayed when you try to turn up an MC ring, you can perform one or both of the following to view information about the problem.

- Select the listed problem and click on the Properties button.
- View the Operational State and Failure Reason fields on the State tab of the MC ring properties form.

The 5620 SAM performs a series of checks to determine whether an MC ring can be turned up. The checks include verifying the following:

- The synchronization tag is configured on the BSA.
- The VLAN-level synchronization tag is valid.
- The IES or VPRN interface for the IB-RCC is configured.
- BFD is enabled on the IB-RCC interface.
- The IES or VPRN interface is operationally up.
- The IB-RCC interface is not in use by another MC ring.
- The IB-RCC interface is on the port used for MC synchronization.
- The IB-RCC destination IP address is configured.
- The IB-RCC destination IP address is not the same as the IB-RCC source IP address.
- The IB-RCC destination IP address is not in the same subnet as the IB-RCC source IP address.
- The MVPLS or VPLS site is not configured as an endpoint for redundant spoke SDPs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Turn up the MC ring using the MC ring properties form.

Note — Using this method enables you to view real-time MC ring status information while the 5620 SAM turns up the MC ring.

i Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

ii Click on the State tab button.

iii Set the Administrative State parameter to Up.

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

vi View the dynamically updated information in the Operational State field.

vii Close the MC Ring (Edit) form.

viii Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

ix Repeat steps 4 a ii to vii.

b Turn up the MC ring using the navigation tree. Perform the following steps.

i Click on the Components tab button.

ii Right-click on the first site object and choose Turn Up from the contextual menu. A dialog box appears.

iii Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

iv Right-click on the second site object and click on the Turn Up button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

5 Close the MC Ring Group (Edit) form.

Procedure 45-5 To view the operational status of MC ring group components

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside a site that hosts an MC ring. The MC Ring (Edit) form opens.

5 Click on the State tab button.

6 View the dynamically updated information in the Operational State field. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Shut Down—the MC ring is administratively down
- Config Error—the MC ring has a configuration error
- No Peer—the peer MC ring is not configured
- Connected—the MC ring is operational
- Broken—the RNCV check fails
- Local Broken—the MC ring site cannot connect to a ring node
- Conflict—the MC ring configuration conflicts with another configuration
- Testing Ring—an RNCV check is in progress
- Peer Down—the peer MC ring site is inoperable
- Waiting For Peer—the peer MC ring site is initializing

7 Click on the Components tab button.

8 Right-click on a ring node object and choose Properties from the contextual menu. The MC Ring Node (Edit) form opens with the General tab displayed.

9 Click on the State tab button.

10 View the dynamically updated information in the Local Operational State and Remote Operational State fields. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Not Provisioned—the ring node configuration is incomplete
- Config Error—the ring node is misconfigured
- Not Tested—no RNCV check result is available
- Testing—an RNCV check is in progress
- Connected—the ring node is operational
- Disconnected—the ring node cannot be reached

11 Close the MC Ring Node (Edit) form.

12 Close the MC Ring (Edit) form.

13 Close the MC Ring Group (Edit) form.

Procedure 45-6 To delete an MC ring group

Caution — Deleting an MC ring group removes all of the child objects that are associated with the MC ring group, such as the following:

- MC rings
- ring nodes

Ensure that you specify the correct MC ring group for deletion in this procedure.

Note 1 — You must set the administrative state of an MC ring to Down before you can delete the MC ring.

Note 2 — Before you can set the administrative state of an MC ring to Down, you must administratively disable each VPLS or MVPLS SAP in the ring, regardless of the path they use.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

5 Click on the State tab button.

6 Set the Administrative State parameter to Down.

7 Click on the Apply button. A dialog box appears.

8 Click on the Yes button. The 5620 SAM shuts down the MC ring.

9 Close the MC Ring (Edit) form.

10 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

11 Repeat steps 5 to 9.

12 Select the MC ring group in the list and click on the Delete button. A dialog box appears.

13 Click on the View Dependencies button. A Warning form opens.

14 View the dependency information.

15 Select the I understand the implications of this action check box.

16 Click on the Yes button. The 5620 SAM deletes the MC ring group and the corresponding configuration on each member site.

17 Close the Manage Node Redundancy form.

Policy management

62 — NAT policies

63 — Format and range policies

46 — Policies overview

46.1 Policies overview

The 5620 SAM supports the template-based creation of rules. These rules are called policies. The types of policies are:

- service management
- routing management
- network management
- 7250 SAS and Telco
- OmniSwitch QoS
- OmniSwitch Ethernet services

A 5620 SAM operator can distribute or delete policies on sites and NEs that are within their span of control.

Policies are global or local in scope. Global policies are created using the 5620 SAM. Local policies are instances of global policies that are assigned to individual NEs. Depending on the distribution mode of a local policy, when you modify a global policy using the 5620 SAM, the local instance is also updated to ensure that the policy instances are synchronized. If a local policy differs from the corresponding global policy because of changes to the global policy, a warning alarm is raised against the local policy. After a global policy is updated and distributed to the participating NEs, the 5620 SAM clears the mismatch alarms associated with the local policy.

To identify local and global policy mismatches, you can perform a policy audit that compares the local and global instances of a policy, and then review the differences. An audit can be performed on local policies of NEs that are in the user span of control and policies that the user license supports.

You can audit all policies in the network or on selected NEs in the following ways:

- by policy group
- by policy type
- by global policy

If there is a mismatch between a local policy instance and the global instance, an alarm is raised against the local policy. The 5620 SAM clears the alarms from previous audits if the mismatch condition no longer exists.

Warning — Alcatel-Lucent recommends that you change a policy on an NE using only the 5620 SAM or an OSS client. This ensures that there is no mismatch in policy IDs or policy configurations between the managed NEs and the 5620 SAM.

Creating or modifying a policy using a CLI may lead to inconsistencies in the policy configuration throughout the network. See Procedure 46-8 for information about identifying policy discrepancies using a policy audit.

Depending on the results of an audit, the mode of the local policy may change. If the audit discovers differences between the local and global policies, you can change the mode to allow only local configuration. When the audit discovers that the local policy and global policy match, the local mode can be changed to synchronize with global policies. For example, when you need the 5620 SAM to discover new NEs, set the mode parameter to local configuration only to ensure that unique policies are not modified when a global policy is updated. The audit results can be reviewed to determine whether a policy should remain local.

The 5620 SAM supports the partial distribution of global policies. Before a global policy is distributed to the NEs, the 5620 SAM determines whether the global policy, policy properties, and the policy entries are applicable for each NE to which the policy is to be applied. If an NE does not support the policy, property, or entry defined in a global policy, the policy is partially distributed to the NE. The inapplicable policy, property, or entry is not distributed to the NE. An alarm is not raised if a policy is partially distributed. When you use the 5620 SAM GUI or OSS, failure of distribution to an NE does not affect distribution to other NEs.

Global policies are created in draft mode. This allows operators to verify that the policy is correctly configured before they distribute the policy to the NEs. The 5620 SAM creates a global policy in draft mode for newly discovered local policies. When the policy is approved for distribution, you can change the mode to released, which also distributes the policy to existing local definitions. The 5620 SAM saves the latest released version of the global policy. You can monitor policy distribution using the Task Manager. See Procedure 3-15 for information about the Task Manager.

When there is no global policy associated with a local policy, the 5620 SAM automatically creates a global policy that is identical to the first discovered local policy. If the local policy is incomplete, the 5620 SAM creates an incomplete global policy. The following read-only parameters describe the initialization phases of a global policy:

- Discovery State
    - In Progress—The global policy is created as part of a specific NE resynchronization during the full NE resynchronization or NE discovery. The global policy does not yet match any local policy and is waiting for completion.
    - Completed—At the end of the full NE resynchronization, when the resynchronization is successful, the global policy is completely updated from the first discovered local policy.
    - Failed—At the end of the full NE resynchronization, if the resynchronization is not successful, the global policy is not updated from the first discovered local policy. A failed global policy is updated during the next successful full NE resynchronization, or the policy can be manually synchronized with a specific local policy. The global policy remains in the Failed state after a 5620 SAM server failure or activity switch.
    - Initialize—The global policy is created by SNMP trap notification. The global policy may need to be manually synchronized with the specific local policy.
    - N/A (default)—The global policy is created or modified by a 5620 SAM user.

- Origin
  - Site ID—The global policy is created as part of a specific NE resynchronization or by SNMP notification.
  - User Name—The global policy is created by a 5620 SAM user.

Note 1 — If you attempt to modify a global policy with an "In Progress" Discovery State, the following occurs:

- When discovery or full resynchronization of the NE is ongoing, the modification fails.
- When discovery or full resynchronization of the NE is completed, modifications using OSS proceed, although a warning appears and allows you to cancel the modification. If the modification is not cancelled, the Discovery State is changed to N/A, and the global policy is not updated to match the local policy.
- When a global policy is modified, the Discovery State is reset to N/A.

Note 2 — At any time during discovery or a full resynchronization, you can use the SyncTo method from OSS or synchronize the global policy from any local policy.

When a discovery or full resynchronization of an NE fails and there is no 5620 SAM server failure or activity switch, all global policies that are waiting for completion are changed to Failed for the Discovery State. If you start another full resynchronization of the failed NE, the 5620 SAM tries again to complete the global policies from the NE that is part of the resynchronization and which has the Failed or In Progress Discovery State. The 5620 SAM also attempts completion of the synchronization of global policies that have a Failed or an In Progress State until a server failure or an activity switch occurs.

Table 46-1 describes the recommended operator actions to recover global policies when the Discovery State remains In Progress or Failed.

Table 46-1 Actions to recover global policies

Discovery State	5620 SAM server failure	NE state	Recovery action
In Progress/Failed	No	Resync Failed	Retry a full resynchronization or synchronization from another local policy
In Progress/Failed	No/Yes	Removed/Unmanaged	Synchronization from another local policy
In Progress/Failed	Yes	Resync Completed	Synchronization from another local policy
In Progress/Failed	Yes	Resync Failed	Retry a full resynchronization and synchronization from another local policy

The 5620 SAM supports the ability to scale policy deployment. If you release a large global policy to multiple NEs using one deployer, you may degrade system performance. An operator can configure the maximum number of objects that a deployer can send. The 5620 SAM uses this value to calculate how many NEs can be deployed per deployer. The default value is 10 000 objects per deployer. Table 46-2 provides an example of possible parameter settings to deploy a global policy that contains 1000 objects.

In the example below, there is one deployer per site. When the parameter setting is less than the number of entries in the policy, the 5620 SAM does not use more than one deployer for one site. If the parameter setting is too high, the 5620 SAM uses one deployer for all sites which may impact system performance. See Procedure 46-10 for more information about configuring the maximum number of objects per deployer.

Table 46-2 Example of policy deployment

Policy distribution maximum number of objects per deployer	number of objects in a global policy	Maximum number of sites per deployer
0	—	All sites
1	—	1 site
500	1000	1 site
1000	1000	1 site
5000	1000	5 sites
10 000	1000	10 sites
100 000	1000	100 sites

Service management policies specify how service traffic is handled by network resources such as interfaces, ports, daughter cards, and circuits. The policies can be used by multiple resources on multiple services. Service management policies include access ingress, access egress, MSAP policies, and network policies.

Routing management policies specify routing configuration according to specifically defined parameters. The 5620 SAM supports the following routing management policy types:

- routing
- MPLS administrative group
- VRRP priority control

Service and routing management policies are globally and seamlessly distributed to devices when they are used by resources on the device. They can also be manually distributed to devices. Subsequent changes to policies are distributed and affect all participating resources. Policy configurations can also be changed locally when you configure a network resource, for example, during service configuration or modification. These changes do not affect the global policy.

Network management policies specify how the 5620 SAM communicates with network resources, handles alarms, manages statistics, and stores information. Examples of network management policies are alarm, mediation, and accounting policies.

7250 SAS and Telco policies specify how 7250 SAS and Telco devices are configured and used to provide BTV VLAN, L2 VPN VLANs, and super-VLAN Internet services.

OmniSwitch QoS and Ethernet service policies specify how OmniSwitch devices are configured and used to provide VLAN and SVLAN services.

Time of day policies consist of time range policies and time of day suite policies. Time range policies specify multiple schedules (start and end dates and times) that you can assign to time of day suites or to ACL filter entries. A time of day suite policy is a collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which a time range policy has been assigned. In addition, you can assign time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

Table 46-3 describes the policies that are configured using the 5620 SAM. Unless otherwise stated in the table, the policies are described in more detail in this volume.

Table 46-3 5620 SAM Policy Types

Policy	Applied to	Description	Menu option
7210 Access Egress	Access port	Defines up to eight forwarding class queues and queue parameters for traffic classification. Defines forwarding class to remarking values. Maps forwarding classes to the queues.	Policies→QoS→SROS QoS→Access Egress→7210 Access Egress. See Procedure 47-5.
7210 Access Ingress	Access SAP	Defines up to 18 forwarding class meters and meter parameters for traffic classification. Defines match criteria to map flows to the meters based on any one of the criteria (IP or MAC).	Policies→QoS→SROS QoS→Access Ingress→7210 Access Ingress. See Procedure 47-2.
7210 Network	Uplink port	Defines ingress Dot1p to forwarding class mapping and profile state. Defines the egress queuing parameters associated with each forwarding class.	Policies→QoS→SROS QoS→Network→7210 Network. See Procedure 47-7.
7210 Network [(1)]	Network port [(1)]	Defines ingress Dot1p or DSCP value mapping to forwarding classes. Defines unicast meters. Only unicast meters with range 1-8 are allowed. Defines the egress forwarding class to Dot1p or DSCP value markings. Remarking of QoS bits.	Policies→QoS→SROS QoS→Network→7210 Network. See Procedure 47-7.

(1 of 7)

Policy	Applied to	Description	Menu option
	Network interface (1)	Defines ingress LSP-Exp value mapping to forwarding classes. Defines forwarding class to meter mapping. Defines unicast or multicast meter. Multicast meters are only supported for interface type policy. Defines the egress forwarding class to LSP-Exp value markings. Remarking of QoS bits.	
7210 Network Queue	Uplink port	Defines forwarding class mappings to network queues and queue characteristics for the queues	Policies→QoS→SROS QoS→Network Queue→7210 Network Queue. See Procedure 47-13.
7210 Port Scheduler	Access and uplink ports	Defines the parameters for the port scheduler	Policies→QoS→SROS QoS→Scheduler→7210 Port Scheduler. See Procedure 47-19.
7210 Slope	Access and uplink ports	Enables or disables the high-slope and low-slope parameters in the egress pool	Policies→QoS→SROS QoS→Slope→7210 Slope. See Procedure 47-9.
7250 SAS and Telco Node QoS Level	7250 SAS and Telco devices and ports	Defines QoS policies applied to a 7250 SAS or Telco device.	Policies→QoS→7250 SAS and Telco QoS. See Procedure 47-35.
7250 SAS and Telco ACL Standard IP	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on IP address and subnet mask matching criteria.	Policies→Filter→7250 SAS and Telco ACL Standard IP Filter. See Procedure 48-4.
7250 SAS and Telco ACL Extended IP	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on several IP matching criteria.	Policies→Filter→7250 SAS and Telco ACL Extended IP Filter. See Procedure 48-5.
7250 SAS and Telco ACL IGMP	7250 SAS and Telco devices and ports	Manages how BTV host devices access multicast BTV streams.	Policies→Filter→7250 SAS and Telco ACL IGMP Filter. See Procedure 48-6.
7250 SAS and Telco ACL MAC	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on MAC matching criteria.	Policies→Filter→7250 SAS and Telco ACL MAC Filter. See Procedure 48-7.
7705 SAR Fabric	Daughter cards on the 7705 SAR	7705 SAR Fabric Profile policies specify the fabric shaping rate (kb/s) to the daughter card in the slot specified by the rate.	Policies→QoS→SROS QoS→7705 SAR Fabric. See Procedure 47-24.
802_1X	Ethernet ports	Defines the RADIUS server authentication policy for Ethernet ports	Policies→Ethernet→802_1x. See Procedure 54-1.
9500 MPR QoS	Access interface	Defines ATM classification, policing, and marking	Policies→QoS→9500 MPR QoS→9500 ATM QoS. See Procedure 47-32.
Accounting	Network interface Access interface Circuit	Manages accounting policies.	Tools→Statistics→Accounting. See the *5620 SAM Statistics Management Guide* for more information.
Access Egress	Access interface	Defines egress classification, policing, shaping, and marking on the egress side of the interface	Policies→QoS→SROS QoS→Access Egress→Access Egress. See Procedure 47-3.

(2 of 7)

Policy	Applied to	Description	Menu option
Access Ingress	Access interface	Defines ingress classification, policing, shaping, and marking on the ingress side of the interface	Policies→QoS→SROS QoS→Access Ingress→Access Ingress. See Procedure 47-1.
ACL IP Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv4 matching criteria	Policies→Filter→ACL IP Filter. See Procedure 48-1.
ACL IPv6 Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv6 matching criteria	Policies→Filter→ACL IPv6 Filter. See Procedure 48-2.
ACL MAC Filter	Access interface Circuit	Controls network traffic into or out of an interface or circuit based on MAC matching criteria	Policies→Filter→ACL MAC Filter. See Procedure 48-3.
Admin Group (MPLS)	MPLS interfaces LSPs LSP paths	Configures MPLS administrative groups and defines the groups to which an MPLS interface, LSP, or LSP path belongs.	Policies→MPLS→ Administrative Group. See Procedure 30-17.
Alarm	Alarm logs Alarms	Defines how the 5620 SAM handles individual incoming alarms, and how alarm logs are created and stored.	Administration→Alarm Settings. See Procedures 37-1, 37-2, 37-3 and 37-7.
ATM QoS	Access interface	Defines ATM ingress and egress classification, policing, shaping, and marking	Policies→QoS→SROS QoS→ATM QoS. See Procedure 47-31.
BGP Peering	Residential subscriber host	Applies BGP peering configuration to residential subscriber host.	Policies→Residential Subscriber. See Procedure 68-10.
Connection Profile	ATM channel	Defines a list of VPI/VCI pairs	Policies→ATM→Connection Profile. See Procedure 57-1.
Diameter	Residential Subscriber	Specifies common diameter protocol parameters to be inherited by associated diameter peers.	Policies→Residential Subscriber. See Procedure 68-11.
Egress Multicast Group	VPLS instance	Creates an EMG to which SAPs can be applied on the access port of a VPLS	Policies→Multicast→Egress Multicast Group. See Procedure 49-1.
Egress Queue Group Template	Access interface	Used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports	Policies→QoS→SROS QoS→Queue Group→Egress Template. See Procedure 47-23.
Ethernet CFM	Ethernet services	Defines the Maintenance Domain for Ethernet services (VPLS, EPIPE, VPRN and IES) including SAP and SDP bindings	Tools→Ethernet CFM→Maintenance Domain. See Procedure 80-1.

(3 of 7)

Policy	Applied to	Description	Menu option
Ethernet Service	SAPs and UNI ports	A SAP is associated with a stacked VLAN service. A SAP profile defines values for ingress bandwidth sharing, rate limiting, customer VLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value). A UNI profile is associated with a UNI port and configures how a variety of protocol control packets are processed on the UNI port. Processing actions include Tunnel, Drop, Peer, and MAC Tunnel.	Policies→Ethernet→AOS Ethernet Service. See Procedures 56-1 and 56-2
File	—	Manages files on the device. See the *5620 SAM Statistics Management Guide* for more information.	Tools→Statistics→File Policies See the *5620 SAM Statistics Management Guide* for more information.
Format Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the text format of names and descriptions of services, LSPs, L2 and L3 access interfaces. Format policies must be associated with users and user groups.	Administration→Format and Range. See Procedure 63-1.
IGMP	Subscriber profile	Associates subscriber profiles with static multicast group and static source IP addresses.	Policies→Residential Subscriber. See Procedure 68-9.
IKE Policy	IPsec tunnels IPsec gateways	Create and configure IKE policies.	Policies→ISA Policies→IKE. See Procedure 35-1.
Ingress Queue Group Template	Access interface	Used for Access Ingress Queue Group creation on Ethernet access ports	Policies→QoS→SROS QoS→Queue Group→Ingress Template. See Procedure 47-22.
ISA-IPSec Transform and IPsec security	IPsec tunnels IPsec security associations IPsec tunnel templates	Create and configure IPsec transform policies and IPsec security policy.	Policies→ISA Policies→IPSec Transform. See Procedures 35-2, 35-4, and 35-5.
ISA-IPSec Static Security Association	OSPFv3 interfaces Virtual links	Create and configure IPsec static security association policies.	Policies→IPSec Static Security Association. See Procedure 35-3.
ISA-IPSec Tunnel Template	IPsec gateways	Create and configure IPsec transform policies.	Policies→IPSec Tunnel Template. See Procedure 35-4.
LSP Template MVPN (MPLS)	P2MP LSPs	Configures and manages P2MP LSPs.	Policies→MPLS→LSP Template MVPN. See Procedure 32-23.
Manage auto tunnel rules	—	Create and configure auto-tunnel rules	Policies→Auto Tunnels→Auto Tunnel Rules. See Procedures 52-2, 52-3, 52-4, 52-5, 52-6, 52-7, 52-8 and 52-9.
Manage rule-based tunnels	—	Create and configure rule-based tunnel policies	Policies→Auto Tunnels→Rule-Based Groups. See Procedure 52-1.
Mediation	5620 SAM	Defines how the 5620 SAM polls the network.	Administration→Mediation. See Procedure 14-4.

(4 of 7)

Policy	Applied to	Description	Menu option
MCFR Ingress QoS Profile	MLFR bundles	Create and configure user-defined ingress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→Ingress QoS Profile. See Procedure 47-42.
MCFR Egress QoS Profile	MLFR bundles	Create and configure user-defined egress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→Egress QoS Profile. See Procedure 47-43.
MC MLPPP Ingress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined ingress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile. See Procedure 47-40.
MC MLPPP Egress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined egress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile. See Procedure 47-41.
MSAP	Capture SAPs L2 access interfaces MSAPs L2 and L3 access interfaces	Specifies how parameters are applied in the creation of an MSAP.	Policies→Residential Subscriber. See Procedure 68-5.
Multicast Package	Broadcast TV VLAN services	Defines the set of broadcast channels that are multicast across a ring group in a BTV VLAN.	Policies→Multicast→Multicast Package. See Procedure 49-9.
Multicast Package	VPLS instance	Assigns a common set of multicast groups to all 7450 ESSs or 7750 SRs in an MVR VPLS.	Policies→Multicast→Multicast Package. See Procedure 49-9.
NAT	Routing instances	Create and configure NAT for use in IES and VPRN services.	Policies→ISA Policies→NAT Policy. See Procedure 62-1.
Named Pool Buffer	Network daughter card and network port	Allows the operator to override the default pool allocation behavior	Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool. See Procedure 47-27. Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool. See Procedures 47-21 and 47-28.
NE Deployment, Backup, Software Upgrade	5620 SAM	Defines how the 5620 SAM communicates with the network.	Administration→NE Maintenance. See Section 23.1 for more information.
Network	Network interface	Defines egress QoS marking and ingress QoS interpretation for traffic on core network IP interfaces	Policies→QoS→SROS QoS→Network→Network. See Procedure 47-6.
Network Queue	Network daughter card Network port	Defines the default burst allocations for queues based on the queue's forwarding class	Policies→QoS→SROS QoS→Network Queue→Network Queue. See Procedure 47-12.
PBB MRP	Ethernet ports	Limits the scope of MMRP advertisements to a specific network domain using ISID-based filters for both the MMRP control plane and the B-VPLS data plane	Policies→Ethernet→PBB MRP. See Procedure 55-1.
Policer Control	Ingress or egress SAPs Subscriber Contexts	Provides control hierarchy for policer objects configured on SAPs or subscriber contexts	Policies→QoS→SROS QoS→Scheduler→Policer Control. See Procedure 47-20.

(5 of 7)

Policy	Applied to	Description	Menu option
Policy Sync Group	AA Group Policy	Designate an AA group policy as the master policy and add one or more AA group policies to Policy Sync Group members. Overwrite or add the contents of the master policy to one or more of its members.	Policies→Policy Sync Group. See Procedure 77-4.
Port Scheduler	Egress ports and channels	Defines hierarchical bandwidth allocation and scheduling at the egress port level.	Policies→QoS→SROS QoS→Scheduler→Port Scheduler. See Procedure 47-18.
PW Template	PE routers used for VPLS services	Enables a VPLS PE router to discover the other PE routers that are part of the same VPLS domain or in another BGP VPLS.	Manage→Service→Service PW Template Policies.
QoS	VLAN and stacked VLAN services	QoS policies are used for traffic prioritization, bandwidth shaping, and Layers 2, 3, and 4 filtering.	Policies→QoS→AOS QoS Policies. See Procedures 47-36, 47-37, 47-38 and 47-39 for more information.
RADIUS Accounting Policy	Subscriber profiles	Sends accounting information to the RADIUS server when a subscriber logs in or logs out of a session	Policies→RADIUS Based Accounting. See Procedure 53-1.
Range Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the ID number range for services, LSPs, L2 and L3 access interfaces. Range policies must be associated with users and user groups.	Administration→Format and Range. See Procedure 63-2.
RCA Audit Policy	VLL, VPLS, and VPRN services and physical links	Associates RCA audit policies to VPRN, VPLS, and VLL services and to physical links.	Policies→Network and Service Audits. See Procedure 81-1.
Remote Network Monitoring	5620 SAM	Maps remote network monitoring events to information alarms in the 5620 SAM GUI.	Tools→Remote Network Monitoring (RMON). See Procedure 60-1.
Routing	Routing instance	Manages route policies.	Policies→Routing→Statement. See Procedure 30-11. Policies→Routing→Prefix List. See Procedures 30-12 and 30-16 Policies→Routing→Community. See Procedures 30-13 and 30-16. Policies→Routing→Damping. See Procedures 30-14 and 30-16. Policies→Routing→AS Path. See Procedure 30-15.
Scheduler	Access ingress interface Access egress interface	Defines hierarchical rate limiting and scheduling to govern queue scheduling	Policies→QoS→SROS QoS→Scheduler→Scheduler. See Procedures 47-15 and Section 64.5. Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler. See Procedure 47-16.

(6 of 7)

Policy	Applied to	Description	Menu option
Shared Queue	Network daughter card	Defines distribution of traffic over core network	Policies→QoS→SROS QoS→Shared Queue. See Procedure 47-14.
Shared Risk Link Group (MPLS)	MPLS interfaces LSP paths	Configures Shared Risk Link Groups and associates the groups to one or more MPLS interfaces.	Policies→MPLS→ Shared Risk Link Group. See Procedures 30-18 and 30-19.
Slope	Access port Network daughter card Network port	Defines RED slope behavior	Policies→QoS→SROS QoS→Slope→WRED Slope. See Procedure 47-8. Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope. See Procedure 47-10.
Subscriber identification	SAP	Associates residential subscriber hosts with subscribers for the allocation of network resources.	Policies→Residential Subscriber. See Procedure 68-15.
Time of Day Suite	Aggregation scheduler policies and L2 and L3 access interfaces	A collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which time range policies have been assigned	Policies→Time of Day→Time Of Day Suite. See Procedure 50-2.
Time Range	Time of day suite policy entries and ACL filter policy entries	Specifies multiple schedules that can be used by time of day suite policies or ACL filter policies	Policies→Time of Day→Time Range. See Procedure 50-1.
VRRP	VRRP instance	Applies a VRRP priority-control policy to non-owner VRRP instances in a virtual router.	Policies→VRRP. See Procedure 51-1.

(7 of 7)

Note

(1) Applies to the 7210 SAS-M24F, Release 1.1 R4 or later, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR].

You can apply policies to resources during service creation or modification. You can also apply policies to resources before or after configuring the service by choosing and modifying the resource from the Manage Equipment or Manage Services form.

Policy distribution

The 5620 SAM supports the template-based creation of rules which are called policies. The types of policies are:

- service management
- routing management
- network management
- 7250 SAS and Telco
- OmniSwitch QoS
- OmniSwitch Ethernet services

Policy overrides

With some policy types, you can use the 5620 SAM to configure a policy override that allows you to change or override the default settings associated with the policy.

For policy types that allow multiple overrides to be configured, the Override Policy Items tab on the policy creation form displays all of the subordinate override policies that are configured on the policy. Each override policy is displayed on their own sub-tabs under the Override Policy Items tab. The override policies that appear on the GUI are dynamic, based on the policy type to be configured.

The following policy types aggregate all subordinate override policies on the Override Policy Items tab.

- SLA Profile policies
- Subscriber Profiles policies
- Port policies
- Services (SAP) policies
- HSMDA Scheduler policies

46.2 Workflow to create and assign policies

1. Create the required policies. Table 46-3 describes the policies that are configured using the 5620 SAM.
2. Distribute the policies. See Procedure 46-1 for more information.

Note 1 — You do not need to explicitly distribute a policy; a policy is distributed to a device when it is assigned to a resource on the device.

Note 2 — When you distribute a policy to a 7705 SAR, all values within that policy must be supported by that 7705 SAR; otherwise, the distribution of the policy to that 7705 SAR is blocked.

3. Assign policies to resources during service configuration or modification. See Chapter 64 for more information.

46.3 Policies procedures

Use the following procedures to perform 5620 SAM policies tasks.

Procedure 46-1 To distribute a policy

Use this procedure to manually distribute policies used by network resources and to configure the distribution mode of local policies. Policies are also distributed to a device when the policy is assigned to a resource on that device.

When you distribute a global policy, local policies using the Sync With Global distribution mode allow the NE to receive the policy.

Note — Local policies using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global policy. You must ensure that the policy distribution mode for the local policy is set to Sync With Global if you want the NE to receive the distribution of a global policy.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to distribute. The appropriate policies manager form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button.

4 Choose the policy or policies that you want to distribute.

5 When the policy is in draft configuration mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing one of the following:

- **a** To release a from a *Policy_Type* Global (Edit) form, click on the Properties button. The *Policy_Type* Global (Edit) form opens.
- **b** To release a policy from a policies manager form, click on the Release button. Go to step 10.
- **c** If the policy has previously been released, go to step 10.

Warning — When you switch the configuration mode of the global policy to released, the policy is distributed to existing local definitions.

6 Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

7 Click on the Yes button. The policy configuration mode changes to Released.

8 View the local policy, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local policy in the list.

9 Close the local policy form.

10 Click on the More Actions button and choose Distribute. The Distribute form opens.

11 Select one or more rows in the Available Nodes list.

12 Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.

13 Click on the Distribute button. The policy is distributed to the site or sites.

A progress bar at the lower right of the GUI displays the overall percentage of distribution progress completion to the selected sites. Distribution states (In Progress, Succeeded, or Failed) for individual sites are shown in the Status column for the Selected Nodes.

Note — Distribution failures are reported in a pop-up message. You can view the error message to determine the cause of the failure and which NE or NEs were affected. Distribution failures are also reported using JMS.

14 Close the Distribute form. The policy manager form reappears.

15 View the devices to which a policy is distributed.

- **i** Choose the policy.
- **ii** Click on the Properties button. The policy form opens.
- **iii** Click on the Local Definitions tab button. The device information for the chosen policy is displayed.

16 Configure the distribution mode of the local definitions by performing the following:

- **i** Click on the More Actions button and choose Distribution Mode. The Distribution Mode - *Policy* form opens.
- **ii** Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.
- **iii** Choose one ore more rows from the Available Nodes list.
- **iv** Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.
- **v** Depending on the distribution mode of the chosen site or sites, perform one of the following steps:
    - Click on the Sync With Global button.
    - Click on the Local Edit Only button.
- **vi** Close the Distribution Mode - *Policy* form. The policy manager form reappears.

17 To distribute additional policies, perform steps 4 to 15.

Procedure 46-2 To modify a policy

Use this procedure to change existing policies and entries within policies using the 5620 SAM client GUI. Alternatively, you can use the CLI. The changes are applied immediately to all resources where the policy is applied.

When you modify policy match criteria, for example, the IP match criteria for an access ingress policy, click on the Refresh button to ensure that the 5620 SAM client GUI displays the latest set of match criteria.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to edit.

The Manage *Policy Type* form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button. A list of search results is displayed on the form.

4 Choose the policy that you want to edit.

5 Click on the Properties button. The policy configuration form opens.

6 Perform one of the following:

a If the configuration mode of the policy is set to Released, go to step 7

b If the configuration mode of the policy is set to Draft, configure the parameters, as required, and go to step 13.

7 Configure the parameters, if required. When you modify the configuration, the 5620 SAM changes the configuration mode of the policy to Draft.

8 When you modify filter entries for policies with filters, click on the appropriate tab button and click on the Refresh button to list the filter entries.

9 Click on the Apply button. A dialog box appears.

10 Click on the Yes button.

11 Perform one of the following steps:

a Compare the global policy with the existing local definitions to verify whether you need to reset the policy configuration to the previously released global policy configuration. Perform steps 8 to 10 of Procedure 46-9.

b Go to step 12.

12 Perform one of the following steps:

a Click on the Action button and choose Reset to Released to reset the global policy configuration to the last released configuration of the policy and to cancel any modifications you entered in step 7. Go to step 15.

b Go to step 13.

13 Click on the Switch Mode button beside the Configuration Mode parameter to release the policy for distribution, if required. A dialog box appears.

14 Click on the Yes button. The policy is distributed to existing local definitions.

15 Click on the Local Definitions tab button to view the local instances of the global policy.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The policy configuration form closes and the policy manager form reappears.

18 Close the policy manager form.

Procedure 46-3 To delete a policy

Each service SAP and network interface is associated, by default, with the appropriate ingress, egress, or network policy (ID 1). You can replace the default policy with a customer-configured policy, but you cannot entirely remove a QoS policy. When you remove a QoS policy from a SAP or IP interface, the policy association reverts to the default policy (ingress or egress policy ID 1). The default policy cannot be deleted.

A QoS, ACL, or an AA transit IP policy cannot be deleted until it is removed from the all SAPs or network ports where it is applied. When a policy is deleted, it is removed from the 5620 SAM, including the database and all devices.

Do not delete a routing policy from an NE that is associated with one or more services. Multiple services on the NE may use the policy.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to delete.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed in the bottom panel of the form.

4 Choose the policy that you want to delete.

5 Click on the Delete button. A dialog box appears.

6 Click on the Yes button. The policy configuration form closes and the policy manager form reappears. The policy is removed from the policy list.

Procedure 46-4 To copy or overwrite a policy

You can copy an existing QoS policy, rename the policy with a new QoS policy ID, or overwrite an existing policy ID.

1 Choose Policies→*QoS*→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to copy or overwrite.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy that you want to copy or overwrite.

5 Click on the Properties button. The Policy Type (Edit) form opens.

6 Click on the Action button and choose Copy. The Policy Type (Create) form opens.

7 Configure the parameters as required.

8 Click on the Ok button. The Policy Type (Create) form closes and the Policy Type (Edit) reappears.

9 Close the Policy Type (Edit) form. The Manage *Policy Type* form reappears. The new policy is displayed in the list.

10 Close the Manage *Policy Type* form.

Procedure 46-5 To synchronize a policy

You can use the synchronize function to specify the local policy entry as global and redistribute it across all deployed associations. For example, if a policy is distributed to a wide range of devices and on one of these devices the policy was changed, you can use the synchronize command to synchronize the policy on the device and on the 5620 SAM. You must then distribute the policy to all participating devices, as described in Procedure 46-1.

Note — When you synchronize a policy that is in draft mode, the policy is not distributed to existing local definitions. When you synchronize a policy that is in released mode, the 5620 SAM sets the policy to draft mode. You must set the Configuration Mode parameter to Released to distribute the policy to existing local definitions. Only local policies that have the Distribution Mode parameter set to Sync With Global are affected.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to synchronize.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy or policies that you want to synchronize.

5 Click on the Synchronize button. The Synchronize form opens.

6 Choose the device to which the policy is to be synchronized from the Available Nodes list.

7 Click on the right arrow button. The chosen device moves to the panel on the right side of the form.

8 Click on the Synchronize button.

9 Click on the Cancel button to close the form.

Procedure 46-6 To perform a policy audit for policy groups and types

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on policy groups and policy types. A policy audit cannot be started when another policy audit is in progress.

Caution — If policy types, global policies are not specified, all policies for which the user has licensing permissions are included in the policy audit.

If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Performing a policy audit may take one or more hours to complete.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Tools→Policies Audit from the 5620 SAM main menu. The Policy Audit - audit status (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences

Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

3 Perform one of the following steps:

   a To choose policy groups and policy types to be included in the audit, go to 4.

   b If all policy groups and policy types are included in the audit, go to step 10 to set which NEs to include in the audit.

   c If all policy groups and policy types and the entire network is included in the audit, go to step 11.

4 Click on the Policy Group Selection tab button.

5 Right-click on the Policy Audit icon and choose Select Policy Groups from the contextual menu. The Select Policy Groups form opens.

6 Select policy groups as required and click on the OK button. The chosen policy group keys appear below the Policy Audit icon.

7 Perform one of the following steps:

   a If all policy types within the selected groups are included in the audit, go to step 10.

   b To choose which policy types within the selected groups are included in the audit, go to step 8.

8 Right-click on a policy group icon and choose Select Policy types from the contextual menu. The Select Policy types - Policy Audit form opens.

9 Select policy types as required and click on the OK button. The chosen policy type icons appear below the Policy Audit icon.

10 Select NEs to include in the audit, if required.

   i Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.

   ii Click on the Add button. The Select Site form opens.

   iii Click on the Search button. A list of NEs is displayed.

   iv Click on the NEs to be included in the audit.

   v Click on the OK button. The Policy Audit *audit_status* (Edit) form refreshes to display a list of NEs.

11 Click on the Start Audit button.

To interrupt the audit while it is in progress, click on the Stop Audit button.

12 Close the Policy Audit form after the audit finishes.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm form to view alarms that are generated as a result of the policy audit.

Note — The distribution mode of a local policy may change depending on the parameters set in step 2.

14 Double-click on the alarm in the alarm form. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 and 12 of Procedure 46-9 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 46-7 To perform a policy audit for multiple global policies with same type

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on one or multiple global policies with the same type. A policy audit cannot be started when another policy audit is in progress.

Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Choose one or multiple policies in the list.

4 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Global Policy Selection tab displayed and the selected policies listed.

5 Click on the Add button. The Select Policies form opens, displaying a list of global policies to be audited.

6 Select a policy or multiple policies in the list.

7 Click on the OK button. The Policy Audit (Edit) form is refreshed with the selected policies.

8 Click on the General tab button.

9 Configure the parameters:

- Include Non Applicable Attributes
- Set to “Local Edit Only” upon finding of differences
- Set to “Sync with Global” upon finding of no differences

Note — The Set to “Local Edit Only” upon finding of differences and Set to “Sync with Global” upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

10 Perform one of the following:

a To audit selected global policies on the entire network, go to step 12.

b To audit selected global policies on selected NEs go to step 11.

11 Select NEs to include in the audit, if required.

i Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.

ii Click on the Add button. The Select Site form opens.

iii Click on the Search button. A list of NEs is displayed.

iv Click on the NEs to be included in the audit.

v Click on the OK button. The Policy Audit (Edit) form refreshes to display a list of NEs.

12 Click on the Start Audit button to proceed with the policy audit.

To interrupt the audit while it is in progress, click on the Stop Audit button.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

14 Double-click on the alarm in the alarm window. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 and 12 of Procedure 46-9 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 46-8 To perform a policy audit for global policy

An audit compares all local policies with the associated global policy. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit cannot be started when another policy audit is in progress.

Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Select a policy in the list.

4 Click on the Properties button. The *Policy_Name* Global Policy (Edit) form opens.

5 Click on the Local Definitions tab button. A list of local policies is displayed.

6 Perform one of the following:

a To audit a specific local policy or a group of local policies, go to step 7.

b If all local policies in the list are included in the audit, go to step 8.

7 Select one or multiple local policies that you want to include in the audit.

8 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Network Element Selection tab displayed and a list of NEs corresponding to the selected local policies.

9 Click on the General tab button.

10 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences

Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

11 Click on the Start Audit button. To interrupt the audit while it is in progress, click on the Stop Audit button.

12 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

13 Double-click on the alarm in the alarm window. The Alarm Info form opens.

14 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

15 Perform steps 8 and 12 of Procedure 46-9 to locate the discrepancies between the local and global policies.

16 Close Global Policy *Policy_type* (Edit) form.

Procedure 46-9 To identify differences between a global and local policy or two local policies

Note — You can cancel the local audit at any time by clicking on the Action button and choosing Local Audit Off on the *Policy_type* (Edit) form.

1 Choose Policies→*Policy_type* from the 5620 SAM main menu, where *Policy_type* is the type of policy that you want to open and search for global and local differences. The Manage *Policy_type* form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Select a device in the list and click on the OK button. The Select a Network Element form closes and the Manage *Policy_type* form is updated with the NE IP address.

5 Click on the Search button. A list of search results is displayed.

6 Choose the local policy that you want to compare with another policy.

7 Click on the Properties button. The *Policy_type* (Edit) form opens.

8 Click on the More Actions button and choose Local Audit On. The Local Audit form opens.

9 From the Policy scope drop-down menu:

a Choose Global and go to step 10.

b Choose Local and perform the following:

i Click the Select button to choose an NE. The Select a Network Element form opens.

ii Select the required NE from the list and click on the OK button. The Select a Network Element form closes and the Local Node IP Address parameter is configured with the address of the selected NE.

10 Click on the OK button. The Local Audit form closes and the appropriate global or local policy opens for comparison, based on your selection in step 9.

11 Perform one of the following steps, as applicable:

a View the differences between the policies by clicking on the tab buttons that are highlighted with an arrow icon to indicate that differences exist on the policy forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

Note — Global policies can be distributed to many varying NE types. Local policy audits are performed based on absolute database records. In some cases, this means that when you audit a local policy, a change may be indicated on the associated global policy that does not apply specifically to this local policy. The changed global property may simply not be relevant to the NE associated with this local policy.

For example, a Subscriber Profile global policy contains an HSMDA QoS tab. If a change has been made to a property on this tab in the global policy, but the local policy you are auditing applies to an NE that does not support HSMDA, then the following will occur. When you perform the local audit against the global policy, the global policy form will indicate that there is a difference between the two by displaying an arrow icon on its HSMDA QoS tab. However, since the local policy's NE does not support HSMDA, the local policy form will not even display an HSMDA tab for you to compare with. Any such indicated global changes are irrelevant to the local policy and can be ignored.

b For certain policy types, you can click on a Tree tab button on the local or global policy form. New items are highlighted in pink text. Modified items in the tree are highlighted in purple text.

12 Close the local and global *Policy_type* (Edit) forms.

Procedure 46-10 To configure the maximum policy objects per deployer

Perform this procedure to specify the maximum number of NEs to which a policy is distributed by one deployer.

1. Log in to the 5620 SAM main server station as the samadmin user.

2. Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3. Create a backup copy of the nms-server.xml file.

4. Open the nms-server.xml file using a plain-text editor.

5. Search for the following XML tag:

   ```
   <policyConfig policyDistributionMaxObjectsPerDeployer="10000"/>
   ```

6. Change the number, as required. A zero value or a negative number specifies one deployer or all sites, respectively. A one value specifies one deployer per site. The default is 10 000. Alcatel-Lucent recommends that you configure the value between 2000 and 100 000.

   If the <numberOfObjectsPerPolicy> is greater than or equal to the <policyDistributionMaxObjectsPerDeployer> one deployer per site is used.

   If the <numberOfObjectsPerPolicy> is less than the <policyDistributionMaxObjectsPerDeployer> the maxNumberOfSitesPerDeployer is calculated by policyDistributionMaxObjectsPerDeployer divided by the numberOfObjectsPerPolicy.

7. Save and close the nms-server.xml file.

47 — QoS policies

47.1 QoS policies overview

QoS policies define how network traffic is shaped and queued on one or more NEs. You can use the 5620 SAM to create QoS policies that regulate data throughput on the following:

- equipment, for example, ports and MDAs
- routing and forwarding points, for example, access and network interfaces

Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS on ingress.

Access ingress policies define ingress service forwarding class queues and map flows to those queues. When an access ingress policy is created, it always has two queues defined that cannot be deleted: one for the default unicast traffic and one for the default multipoint traffic. These queues exist within the definition of the policy. The queues only get instantiated in hardware when the policy is applied to an access interface. In the case where the service does not have multipoint traffic, the multipoint queue is not instantiated.

In the simplest access ingress policy, all traffic is treated as a single flow and mapped to a single queue, and all flooded traffic is treated with a single multipoint queue.

The required access ingress policy elements include:

- a unique access ingress policy ID
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces
- at least one default unicast forwarding class queue
- at least one multipoint forwarding class queue

The optional access ingress policy elements include:

- additional unicast queues up to a total of 8 for each of the 8 forwarding classes
- 8 HSMDA queues that are automatically created when the policy is created; HSMDA queues are only used by HSMDA SAPs
- additional multipoint queues up to 3 per forwarding class for each type of multipoint traffic (broadcast, multicast and destination unknown unicast)
- QoS policy match criteria to map packets to a forwarding class
- A policer to control traffic flow rate.

Each queue can have unique queue parameters to allow individual policing and rate shaping of the flow mapped to the forwarding class. Mapping flows to forwarding classes is controlled by comparing each packet to the match criteria in the policy.

There is one default access ingress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

Note — The 5620 SAM supports the configuration of HQoS scheduling mechanisms. HQoS provides the ability to rate limit across multiple queues from either single or multiple access interfaces for a specific customer. The building blocks for HQoS include access ingress, access egress, and scheduler policies.

See section 64.4 for a sample service configuration using HQoS.

Policy override

You can override some or all settings associated with an access ingress policy on an L2 or L3 access interface, SLA profile, or subscriber profile.

Note — You can override Access Ingress policies that have the Scope parameter set to template. See Procedure 47-1 for more information.

Forwarding classes

The 5620 SAM supports the configuration of eight forwarding classes and class-based queuing or policing on the managed devices. Each forwarding class is only important in relation to other forwarding classes. A forwarding class provides NEs with a method to determine the relative importance of one packet over another packet in a different forwarding class.

Queues are created for a specific forwarding class to determine how the queue output is scheduled into the switch fabric and the type of parameters that the queue accepts. The forwarding class of the packet, and the in-profile and out-of-profile states, determine how the packet is queued and handled at each hop along its path to a destination egress point. Forwarding classes may also be associated with policers instead of queues. Eight forwarding classes are supported. Table 47-1 lists the default definitions for the supported forwarding classes.

Although all forwarding classes support profile marking, it is a good network engineering practise to ensure that all high priority forwarding classes are in-profile (CIR=PIR) and all low priority forwarding classes are out-of-profile (PIR > CIR=0). This way, distinguishing packets as in-profile or out-of-profile only occurs for assured class types.

Table 47-1 Forwarding classes

Forwarding class ID	Forwarding class name	Forwarding class designation	DiffServ name	Class type	Intended
7	Network control	nc	nc2	High priority	For network control traffic
6	High-1	h1	nc1		For a second network control class or delay/jitter sensitive traffic
5	Expedited	ef	ef		For delay/jitter sensitive traffic
4	High-2	h2	h2		For delay/jitter sensitive traffic
3	Low-1	l1	af2	Assured	For assured traffic; default priority for network management traffic
2	Assured	af	af1		For assured traffic
1	Low-2	l2	cs1	Best effort	For best effort traffic
0	be	be			

Forwarding subclasses

You can use forwarding subclasses for additional access ingress packet classification. One or more subclasses can be associated with each forwarding class. The designations for forwarding subclasses are the same as those for the forwarding classes listed in Table 47-1. Each subclass assumes the behavior of its parent forwarding class. and in combination with the forwarding class provides a greater range of access ingress QoS classification possibilities.

Policers

You can add a policer to an access ingress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify how you want to configure the mapping between the ingress traffic and ingress queue. Mapping is optional and can be based on combinations of customer QoS marking (Dot1p, DSCP, EXP, and precedence), and IP criteria or MAC criteria. Table 47-2 describes the options.

Adding an LspExp rule to a policy forces packets that match the specified MPLS LSP EXP criteria to override the existing forwarding class and enqueuing priority, based on the parameters specified in the LspExp rule. This functionality allows geographically distributed ISP sites to establish site-to-site interconnection service through a backbone network using VPLS/VLL. Each ISP site PE router connects to a 7x50 Ethernet L2 SAP in the backbone network, and traffic is encapsulated in a VPLS/VLL service tunnel. A maximum of eight LspExp rules are allowed on a single access ingress policy.

Table 47-2 Access ingress policy traffic mapping configuration options

Tab button	Use
Dot1p	Maps the Dot1p value of the ingress traffic to the ingress queue ID.
Dscp	Maps the DSCP value of the ingress traffic to the ingress queue ID.
LspExp	Maps the EXP value of the ingress traffic to the ingress queue ID.
Precedence	Maps the precedence value of the ingress traffic to the ingress queue ID.
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic to the ingress queue ID.
MAC Match Criteria	Maps the MAC Match Criteria of the ingress traffic and ingress queue ID.

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS on egress.

Access egress policies define egress service queues and map forwarding class flows to queues. In the simplest access egress policy, all forwarding classes are treated like a single flow and mapped to a single queue.

The required access egress policy elements include:

- a unique access egress policy ID
- at least one defined default queue
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces

The optional egress policy elements include:

- additional queues up to a total of 8 separate queues for each of the 8 supported forwarding classes
- IEEE 802.1p priority value remarking based on forwarding class
- A policer to control traffic flow rate

Each queue in a policy is associated with one or more of the supported forwarding classes. Each queue can have its individual queue parameters allowing individual rate shaping of the forwarding classes mapped to the queue. More complex service queuing models are supported, where each forwarding class is associated with a dedicated queue.

The forwarding class determination per service egress packet is determined at ingress. If the packet ingresses the service on the same managed device, the service ingress classification rules determine the forwarding class of the packet. If the packet was received over a service tunnel, the forwarding class is marked in the tunnel transport encapsulation.

There is one default access egress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

Policy override

You can override some or all settings associated with an access egress policy on an L2 or L3 access interface, SLA profile, or subscriber profile. See Procedure 47-44 for more information.

Note — You can override Access Egress policies that have the Scope parameter set to template. See Procedure 47-3 for more information.

Policers

You can add a policer to an access egress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify how you want to configure the mapping between the egress traffic and egress queue. Mapping is optional and can be based on combinations of customer QoS marking (DSCP and precedence), and IP criteria. Table 47-3 describes the options.

Table 47-3 Access egress policy traffic mapping configuration options

Tab button	Use
Dscp	Maps the DSCP value of the ingress traffic to the ingress queue ID.
Precedence	Maps the precedence value of the ingress traffic to the ingress queue ID.
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic to the ingress queue ID.

Network policies

Network policies are applied to network interfaces or access uplink ports and specify QoS on egress and ingress.

On ingress, a network policy maps incoming DSCP and EXP values to forwarding class and profile state for traffic received from the core network. On egress, the policy maps forwarding class and profile state to DSCP and EXP values for traffic to be transmitted into the core network.

Network queue policies

Network queue policies are applied to network ports, uplink ports, or daughter cards.

Network queue policies determine:

- the default burst allocations for queues based on the queue's forwarding class
- the CIR, PIR, and burst size parameters for the queue

You cannot use the same policy on devices of different releases. For example, if the 5620 SAM is managing a Release 8.0 7750 SR and a Release 9.0 7750 SR, you must create two network queue policies and distribute one to the Release 8.0 7750 SR and one to the Release 9.0 7750 SR.

For network egress, a network burst policy is associated with the network port buffer pool. For network ingress, the network burst policy is associated the network ingress buffer pool of the daughter card.

Network queue policies support multipoint queues and a variable number of forwarding classes. When you want to deploy a network queue policy to devices of different types, you may need to create an instance of the policy for each NE type. Policies that are configured for multipoint queues and a variable number of forwarding classes are deployed only to devices that support the functionality. Modification of an existing policy results in automatic deployment to participating NEs, so must be done with consideration of the policy features and devices involved.

Slope policies

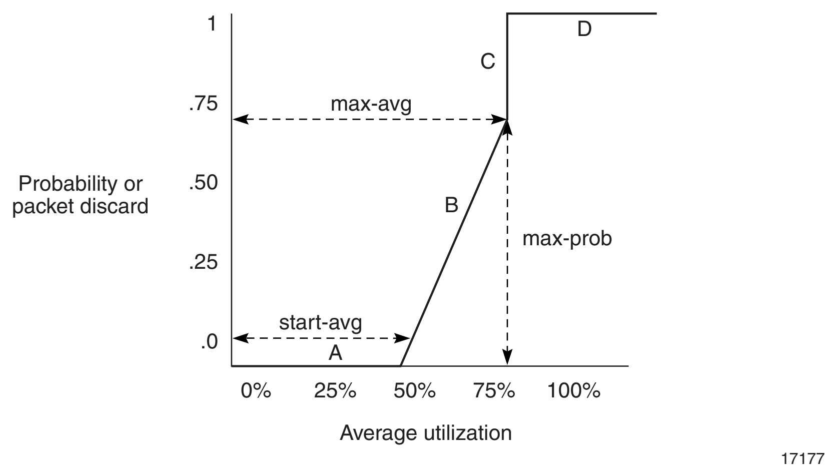
Slope policies are applied to access ports, network ports, and network daughter cards.

Slope policies define weighted RED slope characteristics for buffer pools. Low-priority and high-priority slopes are specified when you configure a slope policy. If a slope policy is not explicitly specified, a default policy is applied.

Each buffer pool supports a high-priority and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for the high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. By default, the high-priority and low-priority slopes are disabled.

A RED slope is a graph with an X (horizontal) and Y (vertical) axis. The X axis plots the percentage of shared buffer utilization, from 0 to 100%. The Y axis plots the probability of packet discard marked from 0 to 1. The slope is defined as four sections, as shown in Figure 47-1.

Figure 47-1 RED slope characteristics



Section A is (0, 0) to (start-avg, 0). For this part of the slope, the packet discard value is always zero, which prevents the RED function from discarding packets when the shared buffer average utilization falls between 1 and start-avg.

Section B is (start-avg, 0) to (max-avg, max-prob). This part of the slope is linear where packet discard probability increases from zero to max-prob.

Section C is (max-avg, max-prob) to (max-avg, 1). This part of the slope shows the instantaneous increase of packet discard probability from max-prob to one. A packet discard probability of one results in an automatic discard of the packet.

Section D is (max-avg, 1) to (100%, 1). On this part of the slope, the shared buffer average utilization value of max-avg to 100% results in a packet discard probability of one.

HSMDA slope policies

The HSMDA slope policy controls the management of the HSMDA queue depth. The polices are applied to queues defined in the SAP ingress and SAP egress QoS to provide congestion control. Congestion control includes a defined maximum depth that the queue can reach when packets and RED of congestion and slope-based discards based on queue depth are accepted.

Note — The 5620 SAM does not support HSMDA slope policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

Shared-queue policies

A shared-queue policy can be applied to daughter cards for optional use by SAPs. The 5620 SAM provides one shared-queue policy for all eight default queues. Each queue is associated with a default forwarding class.

Shared-queue QoS policies can be implemented to facilitate queue consumption on a daughter card; for example, when VPLS, IES, and VPRN services are scaled on one card. Instead of allocating multiple hardware queues for each unicast queue that is defined in an access ingress policy, SAPs with the shared-queuing feature enabled only allocate one hardware queue for each unicast queue.

However, the total amount of traffic throughput at ingress is reduced because ingress packets that are serviced by a shared-queuing SAP are recirculated for additional processing. This can reduce the available bandwidth by half. Shared queuing can also add latency. Network planners should consider these restrictions when they try to scale services on one daughter card.

Table 47-4 lists the queue IDs used by the 5620 SAM to identify the shared-queue types.

Table 47-4 Shared queue types

Shared-queue ID	Shared-queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown

Note — Queue IDs 9 to 32 are also known as multipoint shared queues.

Shared policer output queue

To support hierarchical policing, a default policer-output-queues policy is applied automatically to each IOM that supports ingress policing. In SAM, this shared policer output queue is modeled in the same manner as the existing default shared queue, except that it has only 16 queues.

Multipoint shared-queue policies

Multipoint shared queues minimize the number of multipoint queues that are created for the following:

- ingress VPLS, IES, or VPRN SAPs
- ingress subscriber SLA profiles

Typically, ingress multipoint packets are handled by multipoint queues that are created for each SAP or subscriber SLA profile instance. In some cases, the number of SAPs or SLA profile instances are sufficient for the in-use multipoint queues to represent many thousands of queues on an ingress forwarding plane. If multipoint shared queuing is enabled for the SAPs or SLA profile instances on the forwarding plane, the multipoint queues are not created. Instead, the ingress multipoint packets are handled by the unicast queue that is mapped to the forwarding class of the multipoint packet.

Multipoint shared queues are a superset of shared queuing. With shared queuing on a SAP or SLA profile instance, only unicast packets are processed twice; once for the initial service-level queuing and a second time for switch fabric destination queuing. Shared queuing does not affect multipoint packet handling. Multipoint packet handling in normal service queuing is the same as shared queuing. Shared queuing for unicast packets is automatically enabled when you enable multipoint shared queuing.

The 5620 SAM supports multipoint shared-queue policies for the following services on the 7750 SR, 7450 ESS, 7710 SR:

- Layer 2: VPLS and MVPLS
- Layer 3: IES and VPRN

See the following chapters for more information about enabling multipoint shared queues for a service:

- chapter 71 for VPLS and MVPLS
- chapter 73 for IES
- chapter 74 for VPRN

You can also enable multipoint shared queues in an existing shared-queue policy. See the procedures in this chapter for more information about editing shared-queue policies.

Scheduler policies

Scheduler policies determine the order in which queues are serviced. All ingress and egress queues operate within the context of a scheduler. Multiple queues share the same scheduler. Schedulers control the data transfer between the following queues and destinations:

- service ingress queues to switch fabric destinations
- service egress queues to access egress ports
- network ingress queues to switch fabric destinations
- network egress queues to network egress interfaces

The are two types of scheduler policies:

- single-tier, in which queues are scheduled based on the forwarding class of the queue and the operation state of the queue relative to the queue CIR and PIR
- hierarchical or multi-tier, which allow the creation of a hierarchy of schedules where queues or other schedulers are scheduled by superior schedulers

Scheduler policies are applied to access ingress and access egress interfaces.

Single tier schedulers

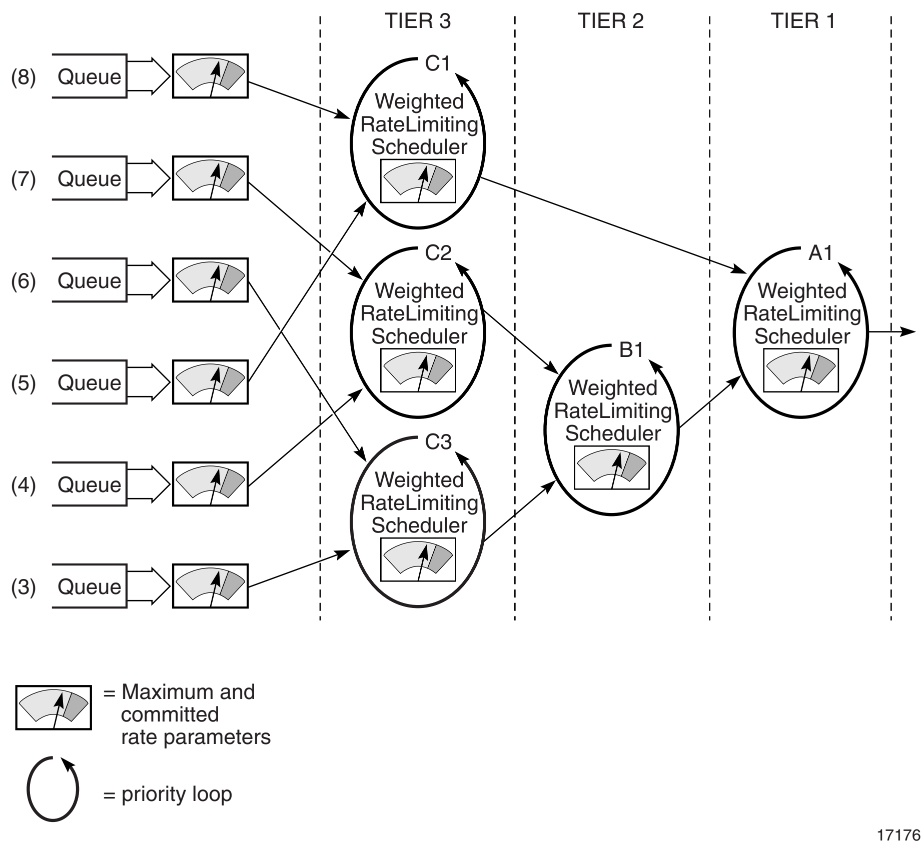
Single-tier scheduling is the default method of scheduling queues. Queues are scheduled with single-tier scheduler policies when no explicit hierarchical scheduler policy is defined or applied. In single-tier scheduling, queues are scheduled based on the forwarding class of the queue and the operational state of the queue relative to the queue CIR and PIR.

Hierarchical schedulers

Hierarchical scheduler policies are used for access ingress and access egress queues. Hierarchical scheduler policies allow you to create a hierarchy of schedulers where queues and other schedulers are scheduled by superior schedulers.

Virtual schedulers are created within the context of a hierarchical scheduler policy. A hierarchical scheduler policy defines the hierarchy and parameters for each scheduler. A scheduler is defined in the context of a tier. The tier level determines the scheduler’s position in the hierarchy. Three tiers of virtual schedulers are supported, as shown in Figure 47-2.

Figure 47-2 Hierarchical scheduler and queue association



Tier 1 schedulers are defined without a parent scheduler. A scheduler can enforce a maximum rate of operation for all child queues and associated schedulers.

You can create a tier 2 scheduler without a parent tier 1 scheduler or a tier 3 scheduler without a parent tier 2 scheduler.

Policy override

You can override some or all settings associated with an ingress or egress scheduler policy on an L2 or L3 access interface or subscriber profile.

HSMDA scheduler policies

The HSMDA scheduler policy controls the scheduling of a set of HSMDA scheduler classes. The policies are assigned to egress HSMDA ports, and the ingress control scheduler between the HSMDA and ingress forwarding plane. The policies assigned to HSMDA egress ports define how all queues associated with the egress port are scheduled. Scheduler policies assigned to the ingress control scheduler between the HSMDA and ingress forwarding plane define how all ingress queues on the HSMDA, regardless of the ingress port, are scheduled.

Note — The 5620 SAM does not support HSMDA scheduler policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

Port scheduler policies

Port scheduler policies determine the virtual scheduling of egress ports by allocating HQoS bandwidth based on the available bandwidth at the egress port level. A port scheduler is defined in the context of a tier. The tier level determines the position of the port scheduler in the hierarchy.

The first tier of the scheduling hierarchy manages the total frame bandwidth that the port scheduler allocates to the eight priority levels. The second tier receives bandwidth from the first tier in two priorities—a within-CIR distribution, and an above-CIR distribution. The within-CIR distribution of the second tier provides bandwidth to the third tier within-CIR distributions for each of the eight priority levels. The above-CIR distribution of the second tier provides bandwidth to the above-CIR distribution of the third tier for each of the eight priority levels.

Up to eight groups can be defined within each port scheduler policy. A group has a rate, an optional cir-rate, and inherits the highest scheduling priority of its member levels. In essence, a group receives bandwidth from the port and distributes it within the member levels of the group according to the weight of each level. Each level will compete for bandwidth within the group based on its weight under congestion situation. If there is no congestion, a priority level can achieve up to its rate (cir-rate) worth of bandwidth. One or more levels can map to the same group.

Note — When the agg-rate-limit is applied to queues of a subscriber which are mapped to different priority levels in the same weighted scheduler group, the bandwidth distribution to the queues will be based on the priority of the level.

Orphan queues or schedulers that are not explicitly associated with the port scheduler receive bandwidth after all parented queues and schedulers are allocated bandwidth.

Port scheduler policies are configured on ports and channels.

Policy override

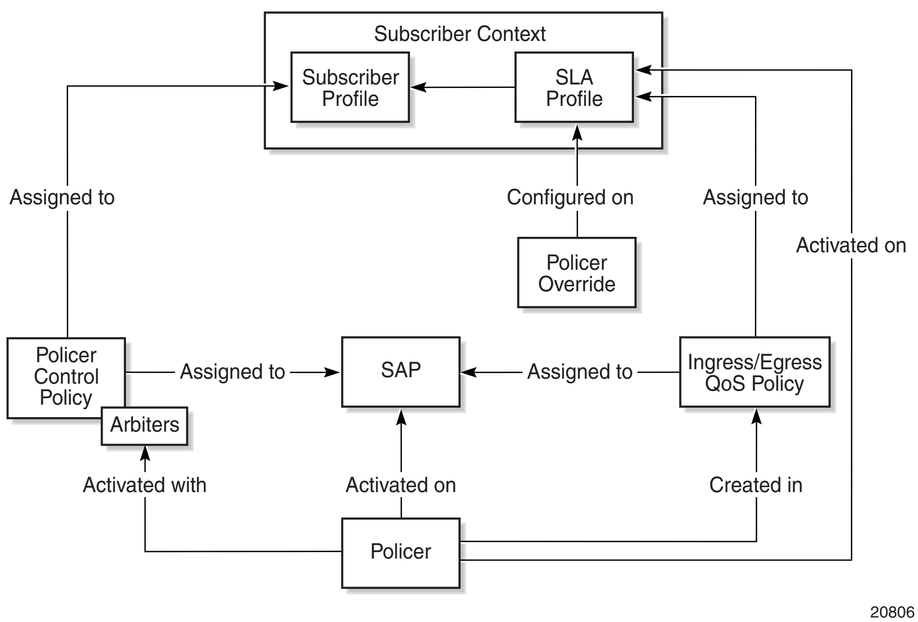
You can override some or all port scheduler settings associated with an access egress queue policy on an L2 or L3 access interface or SLA profile.

Policer control policies

Policer control policies allow you to create a control framework, under which policer objects associated with SAPs or subscriber contexts are configured with traffic control parameters. The policer object is applied to the SAP or subscriber context as part of an access ingress policy or access egress policy. The policer control policy is also applied to the SAP or subscriber context. The policer control policy provides the control framework, and policers are associated with the framework by means of arbiters.

When a policer control policy is applied to a SAP or subscriber context, the system creates a parent policer that is bandwidth limited by the policy's maximum bandwidth rate, as defined under the root arbiter. In addition to the root arbiter, the policy may also contain user defined child arbiters that provide bandwidth control for subsets of child policers.

Figure 47-3 Policer association with SAPs and user contexts under policer control hierarchy



A policer is created as part of an access ingress or access egress policy. The policer is configured with a parent arbiter name. When a policy containing a policer is applied to a SAP, the system scans the available arbiters on the SAP. If an arbiter exists with a name that matches the Parent Arbiter parameter on the policer, a policer to arbiter association is established and the policer becomes part of the policer control hierarchy.

In the case of subscriber contexts, the policer control policy is applied to the sub profile used by the subscriber. The system creates a unique policer control hierarchy for each subscriber associated with the sub profile. An access ingress or access egress policy containing a policer is applied to the subscriber SLA profile. The combination of the sub profile and SLA profile at the subscriber level provides the system with the information required to create the policer control hierarchy instance for the subscriber context.

Section 47.2 shows a sample workflow to configure a policer control hierarchy.

Named buffer pool policies

Named buffer pool policy is a QoS policy used to manage named pools. It allows you to create named pools to override the default buffer pool behavior by creating and allocating ingress and egress queues. Named pools are configured in the named buffer pool policy and are applied at the MDA and/or port ingress and egress level.

Named pools can be further defined in Q1 pools configuration. You can configure and assign queue pools to the following policies:

- Access Ingress
- Access Egress
- Network Queue
- Shared Queue

When a policy is associated at the MDA level, named pools defined in the policy allow queues from any port to be associated. When a policy is associated at the port level, named pools are only available to queues associated with that port. A named pool policy that is currently applied to a MDA or port can be deleted after all association between the policy and the MDA or port have been removed.

When buffer pools are created, renamed or deleted, queues mapped to the pools are moved to default pools. When a queue is moved, traffic that was destined for the queue is temporarily moved to a fail over queue. After the old queue is drained, and the new queue is created and associated with the buffer pool, the saved stats are loaded to the new queue and traffic is moved from the fail over queue to the new queue.

Section 47.3 describes a sample workflow to configure Named Buffer Pools and Q1 pools.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

There are two types of Queue Group Template policies: Ingress Queue Group Template policy and Egress Queue Group Template policy.

- Ingress Queue Group Template policies are used for Access Ingress Queue Group creation on Ethernet access ports
- Egress Queue Group Template policies are used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports

Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

Queue Group Template policies are used in the following network applications:

- Access SAP queue group applications
- Network port queue groups for network interfaces

See chapter 65 for more information about queue groups, the associated network components, and typical applications.

Default policer queue group

The system maintains a special default egress queue group template policy that is applied automatically to all Ethernet ports. The default policer-output-queues policy is configured with two queues:

- Queue 1: configured with a forwarding class value of Best Effort.
- Queue 2: configured with a forwarding class value of Expedite.

All other parameters are default. You cannot delete the default policer-output-queues policy.

7705 SAR fabric profiles

Each daughter card in a 7705 SAR can have two assigned fabric profiles, one for access ingress and one for network ingress. These policies are assigned from the Daughter Card tab of a daughter card slot properties form.

A 7705 SAR fabric profile includes a mode, which cannot be changed after profile creation, and one or more shaping rates. The mode types are Aggregate and Destination. In Aggregate mode, one rate defines the maximum fabric shaping rate that is distributed to each daughter card slot. In Destination mode, there is one fabric shaping rate for each daughter card slot.

In Destination mode, there is also a multi-point shaping rate that is distributed to each daughter card slot.

HSMDA pool policies

The HSMDA pool policy is a QoS policy type that applies to the HSMDA. The policy can be assigned to an ingress or egress HSMDA to control how buffers are distributed between HSMDA queues. HSMDA pool policies do not apply to ports.

Note — The 5620 SAM does not support HSMDA pool policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

ATM QoS policies

ATM QoS policies are used to specify how ATM traffic is managed by using ATM traffic descriptors, such as service category and shaping. You can create up to 2000 ATM QoS policies per router. ATM QoS policies are applied to access interfaces.

Note — For the 9500 MPR (ETSI 1.3), the maximum number of ATM traffic descriptors that are configurable on an NE is 1536, which is twice the maximum number of configurable VPs multiplied by the maximum number of ASAP cards that can be hosted (2x 128 x6).

MC MLPPP ingress and egress QoS profiles

MC MLPPP ingress QoS profiles are used to configure the reassembly timeout for each of the four MLPPP classes. You can create up to 128 ingress QoS profiles per NE.

MC MLPPP egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLPPP classes.

MCFR ingress and egress QoS profiles

MCFR ingress QoS profiles are used to configure the reassembly timeout for each of the four MLFR classes. You can create up to 128 ingress QoS profiles per NE.

MCFR egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLFR classes.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies are used to create and apply QoS policies to these NEs and ports.

Note — The 5620 SAM supports the distribution of policies on the 7450 ESS, 7750 SR, 7710 SR, Release 6.3 or earlier Telco devices, and on the 7250 SAS and 7250 SAS-ES, prior to Release 2.0.

When a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco ACL IGMP packet filter policy entry is created from a multicast package policy, the multicast source IP address is used to specify the multicast source IP address portion of the IGMP packet filter.

OmniSwitch QoS policies

OmniSwitch QoS provides a way to control traffic flows through the switch based on configured policies. The control may be simple such as allowing or denying traffic, or complicated such as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

The OmniSwitch supports the following types of QoS policies:

- basic QoS—to control traffic prioritization and bandwidth shaping
- ACLs—for Layer 2, 3, and 4 filtering

A QoS policy contains a condition and an action. The condition specifies parameters that the switch checks in incoming traffic flows, such as the destination address or ToS bits. The action specifies what the switch does with traffic that matches the condition; for example, the switch may queue the traffic flow with a higher priority or reset the ToS bits.

Ethernet service policies are used to create UNI and SAP profiles. The profiles are applied to stacked VLAN SAPs and UNIs to control traffic and specify options to manage certain traffic types.

7210 SAS QoS policies

The main types of 7210 SAS QoS policies are:

- QoS policies for classification, defining metering and queuing attributes, and marking
- slope policies that define default buffer allocations and RED slope definitions
- port scheduler policies that determine how queues are scheduled

The 5620 SAM supports the following types of 7210 SAS QoS policies:

- 7210 Access Ingress
- 7210 Port Access Egress
- 7210 Access Egress
- 7210 Network
- 7210 Network Queue
- 7210 Slope
- 7210 Queue Management
- 7210 Port Scheduler
- 7210 Remarking
- 7210 MPLS LSP-Exp Map

Table 47-5 lists the types of 7210 SAS QoS policies and describes the policy characteristics.

Table 47-5 7210 SAS QoS policies

Policy type	Applied to	Traffic type affected	Description
7210 Access Ingress	Access port SAP	Ingress	• supports only policing using meters, not rate shaping
7210 Port Access Egress	Access port SAP	Egress	• defines the SLA for service packets as they egress on the SAP
7210 Access Egress	Access port	Egress	• eight queues per port, each forwarding class mapped to a queue • remarking is always turned on • only supports dot1p remarking
7210 Network	Uplink port, network port, or network interface [1]	Ingress and egress	• only supports ingress rate limiting using meters • eight forwarding classes per port • traffic mapping to forwarding classes based on Dot1p, DSCP, or LSP-Exp value markings [2] • supports srTCM, trTCM, trTCM (RFC 2698), and trTCM (RFC 4115)
7210 Network Queue	Uplink port	Egress	• eight hardware queues per port • fixed mapping of forwarding class to queues
7210 Slope	Access or uplink port	Egress	• only supports simple RED • low slope drops out-of-profile packets • high slope drops in-profile packets
7210 Queue Management		Egress	• defines slope parameters that determine a WRED profile for each queue
7210 Port Scheduler	Access or uplink port	Egress	• defines scheduling among the queues and the weight proportion for each queue
7210 Remarking	Access or uplink port	Egress	• configures the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces
7210 MPLS LSP-Exp Map	Network interfaces	MPLS packets	• allows separate mappings of profiles and forwarding classes on network interfaces

Notes

(1) The 7210 SAS-E supports the use of QoS policies on uplink ports. The 7210 SAS-M, Release 1.1 R4 or later, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP support the use of QoS policies on network ports and network interfaces.

(2) Dot1p and DSCP apply only to network ports. LSP-Exp applies only to network interfaces.

See the 7210 SAS-E OS Quality of Service Guide for more information about 7210 SAS QoS and QoS policies.

47.2 Workflow to configure policer control hierarchy

This workflow assumes that the following components already exist:

- a policer control policy
- an access ingress or access egress policy
- a subscriber
- an access interface or SAP

1 Configure arbiters in a policer control policy. See Procedure 47-20 for more information.

i Create arbiters.

ii Configure parent/child relationships between arbiters to build a policer control hierarchy.

2 Configure a policer in an access ingress or access egress policy. See Procedures 47-1 and 47-2 for more information.

i Create a policer to configure traffic control parameters.

ii Assign a parent arbiter to the policer to associate it with the hierarchy configured in the policer control policy.

3 Assign the policer control policy to a subscriber that is configured with an access ingress or access egress policy that includes a policer. See Procedure 68-14 for more information.

4 As required, assign the policer control policy to an access interface or SAP that is configured with an access ingress or access egress policy that includes a policer.

a For an IES L3 access interface, see Procedure 73-1 for more information.

b For an IES SAP, see Procedure 73-8 for more information.

c For a VPLS L2 access interface, see Procedure 71-3 for more information.

d For a VPLS B-L2 access interface, see Procedure 71-13 for more information.

e For a VPLS I-L2 access interface, see Procedure 71-14 for more information.

f For a VPRN L3 access interface, see Procedure 74-2 for more information.

g For a VPRN SAP, see Procedure 74-13 for more information.

47.3 Workflow to configure 5620 SAM named buffer pools

1 Configure a named pool buffer Policy. See Procedure 47-21 for more information.

2 Enable named pool to be configured for a port or MDA. See Procedure 19-18 for more information.

3 Apply a named pool policy to an MDA. See Procedure 19-24 for more information.

4 Apply a named pool policy to a port. See Procedure 20-1 for more information.

5 Configure Q1 pools. See Procedure 47-28 for more information.

6 Assign Q1 pools to access ingress policies. See Procedure 47-1 for more information.

7 Assign Q1 pools to access egress policies. See Procedure 47-3 for more information.

8 Assign Q1 pools to network queue policies. See Procedure 47-12 for more information.

9 Assign Q1 pools to shared queue policies. See Procedure 47-14 for more information.

47.4 QoS policies procedures

This section contains procedures relating to the configuration and maintenance of QoS policies.

Procedure 47-1 To configure an access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→Access Ingress from the 5620 SAM main menu. The Manage Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Access Ingress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Scope
- Priority
- MAC Criteria Type
- Default FC

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 47-1 for more information about forwarding classes.

4 Click on the Queues tab button.

The two default queues that cannot be deleted are displayed—the default unicast traffic queue (ID 1) and the default multipoint traffic queue (ID 11).

i Click on the Create button. The Queue form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multipoint
- Scheduler button
- Mode
- Expedite

Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 47-28.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue (Edit) form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- Rate Type
- Policed
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) are displayed when the Rate Type is not set to kbps.

Ensure that the CIR value is lower than the PIR value.

vii Click on the Burst Size tab button.

viii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Ingress Policy (Create) form reappears.

xi To configure additional queues, return to step i. You can add up to 32 queues.

5 Click on the Policer tab button.

i Click on the Create button. The Access Ingress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the CIR/PIR tab button and configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) are displayed when the Rate Type is set to Percent Local Limit.

Ensure that the CIR value is lower than the PIR value.

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button. The Access Ingress Policer form closes, and the Access Ingress Policy form reappears.

6 Click on the Forwarding Classes tab button. You can create one entry for each of the eight forwarding class types.

i Click on the Create button. The Forwarding Class (Create) form opens with the General tab displayed.

ii Configure the Forwarding Class parameter.

iii Perform any of the following:

- If you need to configure a queue group for some or all traffic types, complete steps iv and v.
- If you need to configure queues for some or all traffic types, complete step v.
- If you need to configure policers for some or all traffic types, complete step v.

iv On the Traffic Control panel, configure the Use Queue Group parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

On the Queues panel, click on the Select button beside the Queue Group Template Policy parameter and select a queue group template policy from the Select Queue Group Template Policy form.

Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID, Multipoint Queue ID, Broadcast Queue ID, and Unknown Queue ID, if selected, are validated against the specified Queue Group Template Policy. When the global policy is distributed to an NE that does not support queue groups, for example, an NE at Release 7.0 R1 or R2, the 5620 SAM ignores the queue group-related parameters. The Queue ID is validated against the local queues for each local policy instance.

v On the Queues panel, configure the parameters:

- Queue ID
  The parameter must be set to a unicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Multipoint Queue ID
  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Broadcast Queue ID
  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Unknown Queue ID
  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.

vi On the Traffic Control panel, configure the Use Policer parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

vii On the Policers panel, for each traffic type configured with the Use Policer parameter, configure the appropriate Policer ID parameter:

- Policer ID
- Multipoint Policer ID
- Broadcast Policer ID
- Unknown Policer ID

Click on the Select button beside each Policer ID parameter and select a policer from the list in the Select Policer form. The policer must be preexisting on the access ingress policy (see step 5).

viii Configure the parameters:

- In Remark
- Out Remark
- In Precedence
  The In Precedence parameter is configurable when the In Remark parameter is set to precedence.
- Out Precedence
  The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.
- In DSCP
  The In DSCP parameter is configurable when the In Remark parameter is set to dscp.
- Out DSCP
  The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.
- Profile
- Mark DE bit 1 as Out of Profile

The Multicast, Broadcast, and Unknown IDs must be set to multicast IDs. The default ID for multicast, broadcast, and unknown queues is 11.

ix Click on the Sub Classes tab button.

x Click on the Create button. The Forwarding SubClass form opens.

xi Configure the parameters:

- Displayed Name
- In Remark
- Out Remark
- In Precedence

  The In Precedence parameter is configurable when the In Remark parameter is set to precedence.
- Out Precedence

  The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.
- In DSCP

  The In DSCP parameter is configurable when the In Remark parameter is set to dscp.
- Out DSCP

  The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.
- Profile
- Mark DE bit 1 as Out of Profile

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The Forwarding SubClasses form closes and the Forwarding Class form reappears.

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Forwarding Class (Create) form closes and the Access Ingress Policy form reappears.

7 Click on the Dot1p tab button.

i Click on the Create button. The Dot1p form opens.

ii Configure the parameters:

- Dot1p
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Dot1p form closes and the Access Ingress Policy form reappears.

8 Click on the DSCP tab button.

i Click on the Create button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the Access Ingress Policy form reappears.

9 Click on the Precedence tab button.

i Click on the Create button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the Access Ingress Policy form reappears.

10 Click on the IP Match Criteria tab button to configure IPv4 match criteria.

i Click on the Create button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Protocol
- Fragment
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the Access Ingress Policy form reappears.

11 Click on the MAC Match Criteria tab button.

i Click on the Create button. The MAC Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Frame Type
- Source MAC
- Mask
- Destination MAC
- ATM VCI
- Mask
- Dot1p
- Mask
- Inner Tag Value
- Inner Tag VID Mask
- Outer Tag Value
- Outer Tag VID Mask
- DSAP
- DSAP Mask
- SSAP
- SSAP Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Destination MAC, Dot1p, and Mask parameters are configurable when the check box for each parameter is selected.

The Inner Tag Value, Inner Tag VID Mask, Outer Tag Value, and Outer Tag VID Mask parameters are configurable when the MAC Criteria Type parameter is set to VID and the Frame Type parameter is set to Ethernet II.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is e802dot2LLC.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP.

The Ether Type parameter is configurable only when the Frame Type parameter value is Ethernet II.

The ATM VCI parameter is configurable only when the Frame Type parameter value is ATM.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The MAC Match form closes and the Access Ingress Policy form reappears.

12 Click on the IPv6 Match Criteria tab button.

i Click on the Create button. The IPv6 Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IPv6 Match form closes and the Access Ingress Policy form reappears.

13 Click on the Lsp Exp tab button.

i Click on the Create button. The Lsp Exp Create form opens.

ii Configure the parameters:

- LspExp
- Forwarding Class
- Priority

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Lsp Exp Create form closes and the Access Ingress Policy form reappears.

14 Click on the Apply button to save the policy. The Access Ingress Policy form is refreshed with additional buttons.

15 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

16 Close the Access Ingress Policy form. The Manage Access Ingress Policies form reappears.

17 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-2 To configure a 7210 SAS access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→7210 Access Ingress from the 5620 SAM main menu. The Manage 7210 Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Access Ingress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Number of Qos Classifiers
- Default FC

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 47-1 for more information about forwarding classes.

4 Click on the Meter tab button.

i Click on the Create button. The Meter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Rate Mode
- MultiPoint

iii Click on the CIR/PIR tab and configure the parameters.

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button.

5 Click on the Forwarding Classes tab button.

i Click on the Create button. The Forwarding Class (Create) form opens.

ii Configure the parameters:

- Forwarding Class
- Meter ID
- Multicast Meter ID
- Broadcast Meter ID
- Unknown Meter ID

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

6 Click on the IP Match Criteria tab button to configure IP match criteria.

i Click on the Create button. The IP Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- DSCP

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

7 Click on the MAC Match Criteria tab button.

i Click on the Create button. The MAC Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Frame Type
- Source MAC
- Mask
- Destination MAC
- Mask
- Dot1p
- Mask
- Ether Type

The Source MAC, Destination MAC, Dot1p, and Mask parameters are configurable when the check box for each parameter is selected.

On 7210 SAS devices, the Frame Type parameter is set to a value of Ethernet II.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

8 Click on the Apply button to save the policy. The 7210 Access Ingress Policy form is refreshed with additional buttons.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the 7210 Access Ingress Policy form. The Manage 7210 Access Ingress Policies form reappears.

Procedure 47-3 To configure an access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→Access Egress from the 5620 SAM main menu. The Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Packet Byte Offset
- Low Burst Max Class

4 If you are creating a 7705 SAR MC MLPPP access egress policy, configure the Use As Multiclass MLPPP Policy For 7705 SAR parameter. Otherwise, go to step 8.

5 Click on the Select button in the WRR Policy panel to choose a WRR policy. The Select WRR Policy search form opens.

6 Select a policy in the list and click on the OK button. The Select WRR Policy form closes and the policy information is displayed on the Access Egress Policy form.

7 Click on the Apply button.

8 Click on the HSMDA Queues tab button. Eight default queues are displayed on the form.

i Select a queue and click on the Properties button. The Access Egress HSMDA Queue (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- Displayed Name
- Description

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Access Egress HSMDA Queue (Create) form.

v Click on the PIR/Burst Size tab button.

vi Configure the parameters:

- PIR (kbps)
- PIR Adaptation
- Maximum Burst Size (bytes)
- Burst Limit (bytes)

You must deselect the associated MAX check box to configure the PIR (kbps) parameter.

You must deselect the associated Default check box to configure the Maximum Burst Size (bytes) or Burst Limit (bytes) parameter.

vii Click on the OK button. The Access Egress Policy (Create) form reappears.

9 Click on the Queues tab button. One default queue is displayed on the form.

i Click on the Create button. The Queue (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Expedite
- Port Average Overhead (%)
- Scheduler button
- Level
- Weight
- CIR Level
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight
- Use WRED Queue
- Packet Byte Offset

Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 47-28.

The Scheduler button, Level, Weight, CIR Level, and CIR Weight parameters in the Parent Scheduler panel are not configurable when the Port Parent parameter in the Port Parent panel is set to true.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) are displayed when the Rate Type is not set to kbps.

vii Click on the Burst Size tab button.

viii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Egress Policy (Create) form reappears.

xi To create additional queues, go to step i. You can create up to eight queues.

10 Click on the Policer tab button.

i Click on the Create button. The Access Egress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the CIR/PIR tab button and configure the parameters:

- Rate Type
- CIR (kbps)
- PIR (kbps)
- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

The CIR (kbps) and PIR (kbps) are displayed when the Rate Type is set to kbps. The CIR (%) and PIR (%) are displayed when the Rate Type is set to Percent Local Limit.

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button. The Access Egress Policer form closes, and the Access Ingress Policy form reappears.

11 Click on the Forwarding Classes tab button.

i Click on the Create button. The Forwarding Class (Create) form opens.

ii Configure the Forwarding Class parameter.

iii Configure the HSMDA Queue ID parameter, if required.

iv Complete one of the following for each Forwarding Class you create:

- If you need to configure a queue from a queue group, set the Traffic Control parameter to the Use Queue Group option and complete steps v and vi, then go to step viii.
- If you need to configure a local queue, set the Traffic Control parameter for the Use Queue option and complete step vi, then go to step viii.
- If you need to configure a policer, set the Traffic Control parameter for the Use Policer option and complete steps v (optionally) and vi (optionally), and then step vii.

v Perform this step only if you intend to use a queue from a queue group. On the Queue Group panel, click on the Select button beside the Queue Group Template Policy parameter. Select the required queue group template policy from the list and click OK.

vi Configure the Queue ID parameter by clicking on the Select button to open the Select Queue - Forwarding Class - Access Egress Policy list form.

The queue you can select here is dependent on your Traffic Control parameter setting, as follows:

- Use Queue: If you specified this, then you can only select one of the locally-defined queues. The local queue in this context is either the default queue or one you created for this policy in step 9. The local queue you select here must be set to a unicast ID. The default ID for unicast queues is 1. Alternatively, you can manually enter 0 if you want the default Queue ID to be used.
- Use Queue Group: If you specified this, then you can only select one of the queues defined in the queue group template policy you chose in step v.

Note — If the Use Queue Group option is enabled for the global policy, then the Queue ID you select is validated against the specified Queue Group Template Policy. If the global policy is distributed to an NE that does not support queue groups, for example, an NE at Release 7.0 R1 or R2, the 5620 SAM ignores the queue group-related parameters. The Queue ID is validated against the local queues for each local policy instance.

- Use Policer: If you specified this, then you can select one of the queues defined in the queue group template policy you chose in step v. If you want to select a local queue instead, then first clear any selection that appears in the Queue Group Template Policy field.

If you are not configuring a policer, proceed to step viii.

vii On the Policers panel, configure the Policer ID parameter by clicking on the Select button. The Select Policer - Forwarding Class - Access Egress Policy list form opens. Select a policer from the list and click OK.

Note — If you specified a local queue Queue ID at step vi, or a queue from the Queue Group Template Policy (steps v and vi) for use with this policer, then traffic will flow through the selected policer and subsequently through the specified queue.

viii Configure the parameters. You can create one entry for each of the eight forwarding class types. The parameters include:

- In Profile
- Out Profile
- In Precedence
- Out Precedence
- In DSCP
- Out DSCP
- Mark DE bit
- Force DE value

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Forwarding Class (Create) form closes and the Access Egress Policy (Create) form reappears with a list of the newly created forwarding classes displayed.

12 Click on the IP Match Criteria tab button.

i Click on the Create button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Protocol
- Fragment
- HSMDA Counter Override
- Forwarding Class
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port
- Profile

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the Access Egress Policy form reappears.

13 Click on the DSCP tab button.

i Click on the Create button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the Access Egress Policy form reappears.

14 Click on the Precedence tab button.

i Click on the Create button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the Access Egress Policy form reappears.

15 Click on the Apply button to save the policy. The Access Egress Policy form is refreshed with additional buttons.

16 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

17 Close the Access Egress Policy form. The Access Egress Policies form reappears.

18 Click on the Search button to display the newly-created policy or policies in the bottom panel of the form.

Procedure 47-4 To configure a 7210 SAS port access egress policy

The 7210 SAS port access egress policy defines the SLA for service packets as they egress on the SAP. Eight queues are defined in the 7210 SAS policy. A 7210 SAS queue management policy can be associated with a queue to manage the buffer allocation for in-profile and out-of-profile packets. A 7210 SAS remarking policy with the type DOT1P or DOT1P-LSP-EXP SHARED can be associated with a 7210 SAS port access egress policy. The 7210 SAS port access egress policy can be associated with an Epipe or VPLS SAP.

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 Port Access Egress from the 5620 SAM main menu. The Manage 7210 Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Port Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Remarking Type
- Egress Remark

The Remarking Type parameter is only configurable on a 7210 SAS-M Release 4.0 R1 and later.

4 If working on a 7210 SAS-X Release 4.0 R1 and later, bind a Remarking Policy:

i Click on the Select button in the Remarking Policy panel to choose a remarking policy. The Select Remarking Policy form opens.

ii Choose a remarking policy in the list and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

5 Click on the Queues tab button. Eight default queues are displayed on the form.

i Choose a queue and click on the Properties button. The PortAccessEgressQueue (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description

iii Click on the CIR/PIR tab button.

iv Configure the parameters:

- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

v Click on the OK button. A dialog box appears.

vi Click on the OK button.

6 Click on the Forwarding Classes tab button.

i Click on the Create button. The 7210 Network Egress Forwarding Class form opens.

ii Configure the parameters. You can create one entry for each of the eight forwarding class types.

- Forwarding Class
- In Profile
- Out Profile
- DSCP In Profile
- DSCP Out Profile

The DSCP In Profile and DSCP Out Profile parameters are only configurable on a 7210 SAS-M Release 4.0 R1 and later

iii Click on the OK button to close the 7210 Network Egress Forwarding Class (Create) form. A dialog box appears.

iv Click on the OK button.

v Repeat steps 6 i to 6 iv if you need to create additional rules. You can configure up to eight rules for one policy.

7 Click on the Apply button to save the policy. The 7210 Port Access Egress Policy form is refreshed with additional buttons.

8 Close the 7210 Port Access Egress Policy form. The Manage 7210 Port Access Egress Policies form reappears.

9 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

Procedure 47-5 To configure a 7210 SAS access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 Access Egress from the 5620 SAM main menu. The Manage 7210 Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Remarking

4 Click on the Select button in the Remarking Policy panel to choose a remarking policy. The Select Remarking Policy form opens.

5 Choose a remarking policy in the list and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 Click on the Queues tab button. Eight default queues are displayed on the form.

i Choose a queue and click on the Properties button. The QueueEntry - 7210 Access Egress Policy (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- ID
- Displayed Name
- Description
- Port Parent
- Weight
- CIR Level

iii Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

iv Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the information is displayed.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button.

7 Click on the Apply button to save the policy. The 7210 Access Egress Policy form is refreshed with additional buttons.

8 Close the 7210 Access Egress Policy form. The Manage 7210 Access Egress Policies form reappears.

9 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

Procedure 47-6 To configure a network policy

1 Choose Policies→QoS→SROS QoS→Network→Network from the 5620 SAM main menu. The Manage Network Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Auto-Assign ID
- Default FC
- Default FC Profile
- LER Use DSCP
- Remark
- Force DSCP Remark

The Force DSCP Remark Remark parameter is set to true.

4 Click on the Egress Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 47-1, are displayed on the form. Configure the forwarding class parameters as required.

5 Double-click on a forwarding class. The network forwarding class form opens.

6 Configure the parameters:

- Use Queue Group
- Queue ID
- DSCP In Profile
- LSP Exp In Profile
- Dot1p In Profile
- Mark DE bit
- DSCP Out Profile
- LSP Exp Out Profile
- Dot1p Out Profile
- Force DE value

The Queue ID parameter is configurable only if the Use Queue Group is enabled. The Queue ID must be specified in the queue group template policy.

Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID is validated against the specified Queue Group Template Policy. When the global policy is distributed to an NE that does not support queue groups, for example, an NE at Release 7.0 R1 or R2, the 5620 SAM ignores the queue group-related parameters.

7 Click on the OK button. The Forwarding Class (Create) form closes and a dialog box appears.

8 Click on the OK button. The Forwarding Class (Create) form closes and the Network Policy (Create) form reappears.

9 Specify how you want to configure the mapping between the ingress traffic and ingress queue by clicking on the appropriate tab button. Mapping is optional and can be based on combinations of customer QoS marking for LSP EXP Bits and Ingress DCSP. Table 47-6 describes the options.

Table 47-6 Network policy traffic-mapping configuration options

Tab button	Use
Ingress LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic to the ingress queue ID.
Ingress DCSP	Maps the DSCP of the ingress traffic to the ingress queue ID.
Ingress Dot1p	Maps the Dot1p tag of the ingress traffic to the ingress queue ID.

Perform the following substeps for each mapping that you want to configure.

i Click on the appropriate tab button.

ii Click on the Create button. A Create form opens.

iii Configure the parameters:

- LSP Exp
- DSCP
- Dot1p
- Forwarding Class
- Profile

The Forwarding Class and Profile parameters appear on all forms. The LSP Exp, DSCP, and Dot1p parameters appear only on the form with the same name as the parameter.

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

10 Click on the Apply button to save the policy. The Network Policy form is refreshed with additional buttons.

11 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Close the Network Policy form. The Manage Network Policies form reappears.

13 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-7 To configure a 7210 SAS network policy

The network QoS policy consists of an ingress and egress component. The ingress component defines how Dot1p, DSCP, or LSP-Exp bits are mapped to an internal forwarding class and a profile state. The ingress component also defines how the forwarding classes are mapped to meters, and defines the meters of the QoS. The egress component performs remarking, which is enabled by default but can be configured. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy.

1 Choose Policies→QoS→SROS QoS→Network→7210 Network from the 5620 SAM main menu. The Manage 7210 Network Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Nw Mgr ID
- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Type
- Default FC
- Default FC Profile
- Remarking

4 Click on the Select button in the Remarking Policy panel. The Select Remarking Policy form opens.

5 Choose a remarking policy and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 If configuring a Network Interface type Network Policy on a 7210 SAS-M Release 4.0 R1 and later, or a 7210 SAS-X Release 4.0 R1 and later, perform the following:

i Configure the Meter Color Mode parameter.

ii Click on the Select button in the MPLS EXP-LSP Profile panel. The Select MPLS LSP-EXP Profile form opens.

iii Choose an MPLS LSP-EXP Profile and click on the OK button. The Select MPLS LSP-EXP Profile form closes and the information is displayed.

7 Click on the Egress Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 47-1, are displayed on the form. Configure the forwarding class parameters, as required.

8 Double-click on a forwarding class. The 7210 Network Egress Forwarding Class (create) form opens.

9 Configure the parameters:

- Dot1p In Profile
- Dot1p Out Profile
- LSP Exp In Profile
- LSP Exp Out Profile
- DSCP In Profile
- DSCP Out Profile

Note — The 7210 SAS-M Uplink access node does not support DSCP In Profile and DSCP Out Profile in Egress Forwarding Classes.

10 Click on the OK button. The 7210 Network Egress Forwarding Class (create) form closes and a dialog box appears.

11 Click on the OK button.

12 Configure the mapping between the ingress traffic and ingress queue by clicking on the appropriate tab button. Table 47-7 describes the options.

Table 47-7 7210 SAS network policy traffic-mapping configuration options

Tab button	Use
Ingress LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic to the ingress queue ID.
Ingress DSCP	Maps the DSCP of the ingress traffic to the ingress queue ID.
Ingress Dot1p	Maps the Dot1p tag of the ingress traffic to the ingress queue ID.

Perform the following substeps for each mapping that you want to configure.

i Click on the appropriate tab button.

ii Click on the Create button. A Create form opens.

iii Configure the parameters:

- LSP Exp
- DSCP
- Dot1p
- Forwarding Class
- Profile

The Forwarding Class and Profile parameters appear on all forms. The LSP Exp, DSCP, and Dot1p parameters appear only on the form with the same name as the parameter.

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

13 Repeat step 12 for each new rule that you need to add. You can configure up to eight rules.

14 Click on the Ingress Meter tab button.

15 Click on the Create button. The Network Ingress Meter (Create) form opens with the General tab displayed.

16 Configure the parameters:

- ID
- MultiPoint
- Mode

Note — The 7210 SAS-M Uplink access node supports ingress meters from 1 to 12 and the Multipoint is set to true.

17 Click on the CIR/PIR tab button.

18 Configure the parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

19 Click on the Burst Size tab button.

20 Configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

21 Click on the Apply button. A dialog box appears.

22 Click on the OK button.

23 Repeat steps 16 to 22 if you need to create additional ingress meter rules.

24 Click on the Cancel button to close the NetWork Ingress Meter (Create) form.

25 Click on the Ingress FCMeter tab button.

26 Click the Create button. The 7210 Network Ingress Forwarding Class (Create) form opens.

27 Configure the parameters:

- Forwarding Class
- Meter
- MultiCast-Meter

Note — The MultiCast-Meter option is supported for the 7210 SAS-M Uplink access node. Meters range from 1 to 12.

28 Click on the Apply button. A dialog box appears.

29 Click on the OK button.

30 Repeat steps 27 to 29 to add additional forwarding class mapping rules.

31 Click on the Cancel button to close the 7210 Network Ingress Forwarding Class (create) form.

32 Click on the Apply button. A dialog box appears.

33 Click on the OK button.

34 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

Procedure 47-8 To configure a WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→WRED Slope from the 5620 SAM main menu. The Manage Slope Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The Slope Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

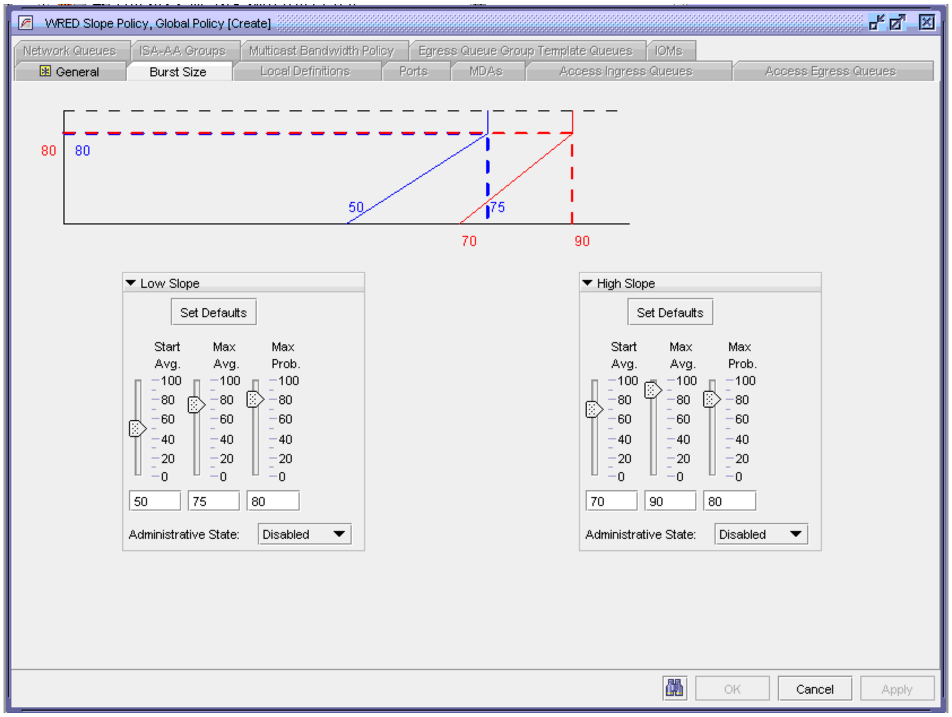
- Displayed Name
- Description
- Time Average Factor (weight)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

When packets are queued, shared buffer average utilization is calculated using the Time Average Factor for the buffer pool. The time average factor specifies the weighting between the previous shared buffer average utilization result and the new shared buffer utilization to determine the new shared buffer average utilization.

4 Click on the Burst Size tab button. The Burst Size form opens, as shown in Figure 47-4.

Figure 47-4 Slope policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Average
- Max Avg.
- Max Prob.
- Administrative State

6 Click on the Apply button to save the policy. The Slope Policy form is refreshed with additional buttons.

7 Click on the Action button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

8 Close the Slope Policy form. The Manage Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-9 To configure a 7210 SAS slope policy

The 7210 SAS supports SRED queue management. Default buffer pools are associated with each port. Each port has two associated buffer pools:

- access egress pool
- access uplink egress pool

Each pool is associated with a default slope policy that disables the low and high slopes within the pool.

1 Choose Policies→QoS→SROS QoS→Slope→7210 Slope from the 5620 SAM main menu. The Manage 7210 Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Slope Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — You cannot use a colon in the Displayed Name value. The 5620 SAM uses colons as separators for the object full name.

4 If you are configuring a 7210 SAS-D 6F 4T ETR, go to step 7.

5 Click on the Burst Size tab button.

6 Configure the Low Slope and High Slope parameters:

- Administrative State
- Start Threshold
- Queue1 Drop Rate
- Queue2 Drop Rate
- Queue3 Drop Rate
- Queue4 Drop Rate
- Queue5 Drop Rate
- Queue6 Drop Rate
- Queue7 Drop Rate
- Queue8 Drop Rate

7 Click on the Queue Slope tab button. Eight default queues are displayed on the form.

8 Choose a queue and click on the Properties button. The QueueSlope, 7210 Slope Policy (Create) form opens.

9 Configure the Time Average Factor parameter.

10 Configure the parameters for the high slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

11 Configure the parameters for the low slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

12 Configure the parameters for the non-TCP slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The QueueSlope, 7210 Slope Policy (Create) form closes.

15 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

16 Close the Slope Policy form. The Manage 7210 Slope Policies form reappears.

17 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-10 To configure an HSMDA WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope from the 5620 SAM main menu. The Manage HSMDA Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Slope Policy (Create) form opens with the General tab displayed.

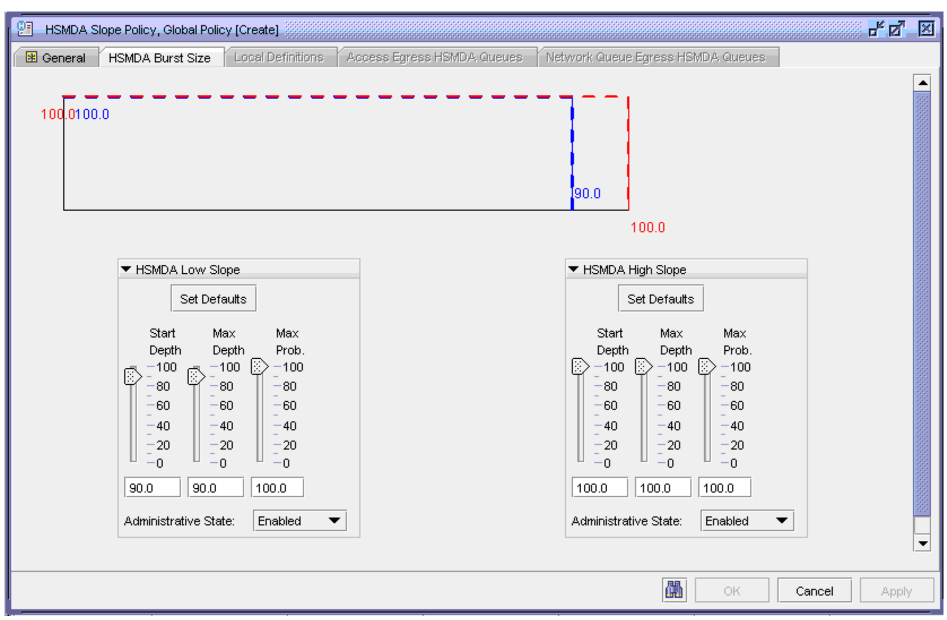
3 Configure the parameters:

- Displayed Name
- Description
- Queue MBS (bytes)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Burst Size tab button. The Burst Size form opens, as shown in Figure 47-5.

Figure 47-5 HSMDA Slope Policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Depth
- Max Depth
- Max Probability
- Administrative State

6 Click on the Apply button to save the policy. The HSMDA Slope Policy form is refreshed with additional buttons.

7 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

8 Close the HSMDA Slope Policy form. The Manage HSMDA Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-11 To configure a 7210 SAS queue management policy

Use a 7210 SAS queue management policy to configure slope parameters that specify a WRED profile for each queue. WRED is used to manage buffers during periods of congestion.

Note 1 — You can assign a 7210 SAS queue management policy to the queues of the following 7210 SAS policies:

- network queue policy
- access egress policy

Note 2 — You cannot modify a default 7210 SAS queue management policy.

1 Choose Policies→QoS→SROS QoS→Slope→7210 Queue Management from the 5620 SAM main menu. The Manage 7210 Queue Management Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Queue Management Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Scope
- Time Average Factor

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the parameters for the burst size:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

5 Configure the parameters for the high slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

6 Configure the parameters for the low slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

7 Click on the Apply button. The 7210 Queue Management Policy (Edit) form is refreshed with additional tab buttons.

8 Click on the following tab buttons to view information about a 7210 SAS queue management policy:

- Network Queues
- SAP Egress Queues
- Local Definitions
- Tree
- Faults

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the 7210 Queue Management Policy form. The Manage 7210 Queue Management Policies form reappears.

11 Click on the Search button to display the newly created policies in the bottom panel of the form.

Procedure 47-12 To configure a network queue policy

You cannot use the same policy on devices of different releases. For example, if the 5620 SAM manages a Release 8.0 7750 SR and a Release 9.0 7750 SR, you must create two network queue policies and distribute one to the Release 8.0 7750 SR and one to the Release 9.0 7750 SR.

1 Choose Policies→QoS→SROS QoS→Network Queue→Network Queue from the 5620 SAM main menu. The Manage Network Queue Policies form opens.

2 Perform one of the following:

  a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

  b Click on the Create button. The Network Queue Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

  - Displayed Name
  - Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the Packet Byte Offset parameter in the Egress HSMDA panel.

5 Click on the Select button in the WRR Policy panel to choose a WRR policy. The Select WRR Policy search form opens.

6 Select a policy in the list and click on the OK button. The Select WRR Policy form closes and the policy information is displayed on the Network Queue Policy form.

7 Click on the Apply button.

8 Click on the Egress HSMDA Queues tab button. Eight default queues are displayed on the form.

9 Double-click on a queue in the list to configure a default Egress HSMDA queue. The Network Queue Egress HSMDA Queue (Edit) form opens with the General tab displayed.

10 Configure the WRR Weight parameter.

Note — The WRR Weight parameter is only displayed and configurable for Egress HSMDA Queues 1, 2, and 3.

11 Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

12 Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Network Queue Egress HSMDA Queue form.

13 Click on the PIR/Burst SIze tab button.

14 Configure the parameters:

- PIR (%)
- PIR Adaptation
- Maximum Burst Size (bytes)
- Burst Limit (bytes)

You must deselect the associated Default check box to configure the Maximum Burst Size (bytes) or Burst Limit (bytes) parameter.

15 Click on the OK button. The Network Queue Egress HSMDA Queue configuration form closes and the Network Queue Policy (Create) form reappears with a list of the Egress HSMDA Queues displayed.

16 Click on the Queues tab button. Two default queues are displayed on the form.

17 Perform one of the following:

a To configure a default queue, double-click on a queue in the list. The Entry, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new queue, click on the Create button. The Entry, Network Queue Policy (Create) form opens with the General tab displayed.

18 Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multipoint
- Expedite
- Port Average Overhead (%)
- Port Parent
- Level
- CIR Level
- Weight
- CIR Weight

19 Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

20 Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Network Queue Policy form.

21 Click on the CIR/PIR tab button.

22 Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

23 Click on the Burst Size tab button.

24 Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The Entry, Network Queue Policy configuration form closes and the Network Queue Policy (Create) form reappears with a list of the network queues displayed.

27 Click on the Forwarding Classes tab button.

28 Perform one of the following:

a To configure an existing forwarding class, click the Search button and then double-click on a forwarding class in the list. The Forwarding Class, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new forwarding class, click on the Create button. The Forwarding Class, Network Queue Policy (Edit) form opens.

29 Configure the parameters:

- Forwarding Class
  The Forwarding Class parameter can be configured only when you are creating a forwarding class network queue policy.
- Queue ID
- Multipoint Queue ID
- Egress HSMDA Queue ID

30 Click on the OK button to close the forwarding class configuration form.

31 Click on the OK button in the dialog box that appears.

32 Click on the Apply button.

33 Click on Yes in the dialog box that appears.

34 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. The Distribute - Network Queue form opens.

> **Note 1 —** When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.
>
> **Note 2 —** Policies are also automatically distributed to devices when they are used by resources on the device.
>
> **Note 3 —** The 5620 SAM automatically distributes an updated policy to a device when the policy is in use on the device.

i Select the devices in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The devices move to the Selected Nodes panel.

ii Click on the Distribute button. The Distribute - Network Queue form closes.

When the Policy has been successfully distributed, the selected devices will appear on the list under the Local Definitions tab button.

35 Policy parameters for a specific local device can be modified by selecting the device from the Local Definitions list and clicking on Properties. The Network Queue Policy (Edit) form for the device opens. Any changes you make here will only affect the selected device.

36 Click OK to close the Network Queue Policy form. The Manage Network Queue Policies form reappears.

37 Click on the Search button to display the newly-created policy or policies in the list panel of the form.

Procedure 47-13 To configure a 7210 SAS network queue policy

1 Choose Policies→QoS→SROS QoS→Network Queue→7210 Network Queue from the 5620 SAM main menu. The Manage 7210 Network Queue Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Network Queue (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Click on the Queues tab button. Eight default queues are displayed on the form.

5 Double-click on a queue in the list. The NQueueEntry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

8 Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the information is displayed.

9 Configure the parameters in the Port Parent panel:

- Port Parent
- Weight
- CIR Level

10 Click on the CIR/PIR tab button.

11 Configure the parameters:

- CIR (%)
- CIR Adaptation
- CIR (%)
- PIR Adaptation

12 Click on the OK button. The NQueueEntry (Create) form closes and a dialog box appears.

13 Click on the OK button. The 7210 Network Queue (Create) form reappears with a list of the network queues displayed.

14 Click on the Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 47-1, are displayed on the form.

15 Click on the Cancel button to close the NQueueForwardingClass (View) form.

16 Click on the OK button to save the settings and close the 7210 Network Queue (Create) form.

17 Click on the Distribute button to manually distribute the policy locally to devices. The Distribute - Network Queue for 7210 form opens.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

18 Click on the Apply button.

19 Close the Manage 7210 Network Queue Policies form.

Procedure 47-14 To modify a shared-queue policy

You cannot create shared-queue policies. Instead, you modify the existing default policy (default or policer-output-queues). Modification of shared-queue policies is supported on the 7750 SR and 7450 ESS.

Table 47-8 shows the default queue number, forwarding class, PIR, CIR, and CBS values for each shared queue.

Table 47-8 Shared queue default values

Queue #	FC	PIR (%)	CIR (%)	High priority reserved	CBS (%)	MBS (%)
1	be	100	0	10	3	25
2	l2	100	25	10	3	25
3	af	100	20	10	3	25
4	l1	100	25	10	10	50
5	h2	100	100	10	10	50
6	ef	100	100	10	10	50
7	h1	100	10	10	3	50
8	nc	100	10	10	1	50

The default behavior automatically chooses the expedited or non-expedited nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1 or h2), the queue is treated as an expedited queue by the hardware schedulers. When any non-expedited forwarding classes are mapped to the queue (be, af, l1 or l2), the queue is treated as best effort (be) by the hardware schedulers.

1 Choose Policies→QoS→SROS QoS→Shared Queue from the 5620 SAM main menu. The Manage Shared Queue Policies form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. The default shared-queue policy is listed.

4 Choose the policy in the list and click on the Properties button. The Shared Queue Policy (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Queues tab button.

Table 47-9 list the queue IDs that are used by the 5620 SAM to identify the shared queue types.

Table 47-9 Shared queue types

Shared queue ID	Shared queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown

There are 32 default queues are displayed on the form. Configure the queues as required. Only 16 queues are available for the policer-output-queues policy.

i Double-click on a queue in the list. The Queue configuration form opens with the General tab displayed.

ii Configure the Expedite and Pool Name parameters.

Note — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 47-28.

iii Click on the CIR/PIR tab button.

iv Configure the parameters:

- CIR (%)
- PIR (%)

v Click on the Burst Size tab button.

vi Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

vii Click on the OK button. The queue configuration form closes and a dialog box appears.

viii Click on the OK button.

7 Click on the Forwarding Classes tab button.

Eight default objects based on the eight forwarding classes, as described in Table 47-8, are displayed on the form. You cannot associate different forwarding classes with the shared queues.

8 Click on the L2 Interfaces or L3 Interfaces tab button. (Applies to default shared queue policy only.)

9 Select an interface in the list and click on the Properties button. The L2 or L3 Access Interface form opens with the General tab displayed.

10 Click on the QoS tab button. (Applies to default shared queue policy only.)

11 Configure the Use Multipoint Shared Queue parameter.

12 Click on the OK button. The Shared Queue Policy form reappears.

13 Click on the Apply button to save the policy. The Shared Queue Policy (Edit) form refreshes.

To modify a local instance of the shared-queue policy, complete steps 1 to 5. Click on the Local Definitions tab. The shared-queue policies for each managed device are listed. Select a shared-queue policy in the list and click on the Properties button to modify the local instance of the policy. Complete steps 6 to 13.

Procedure 47-15 To configure a scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Scheduler from the 5620 SAM main menu. The Manage Scheduler Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

   b Click on the Create button. The Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Frame Based Accounting

4 Click on the Apply button.

5 Click on the Schedulers tab button.

   The scheduler defines bandwidth control that limits each child (other schedulers and queues) that are associated with the scheduler.

6 Click on the Create button. The Entry, Scheduler Policy (Create) form opens.

7 Configure the parameters:

- Displayed Name
- Description
- Tier

  The Tier parameter identifies the level of hierarchy with which a group of schedulers is associated. A parent is tier 1. Children are tier 2. Grandchildren are tier 3. You can create a tier 2 child scheduler without creating a parent tier 1 scheduler, and you can create a grandchild tier 3 scheduler without creating a child tier 2 scheduler.
- Summed CIR
- PIR (kbps)
- CIR (kbps)
- Parent Scheduler

  Click on the Select button to display a list of valid parent schedulers.
- Level
- CIR Level
- Weight
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight

The Parent Scheduler, Level, CIR Level, Weight, and CIR Weight parameters appear only when the Tier parameter is set to 2 or 3 and the Port Parent parameter is set to false.

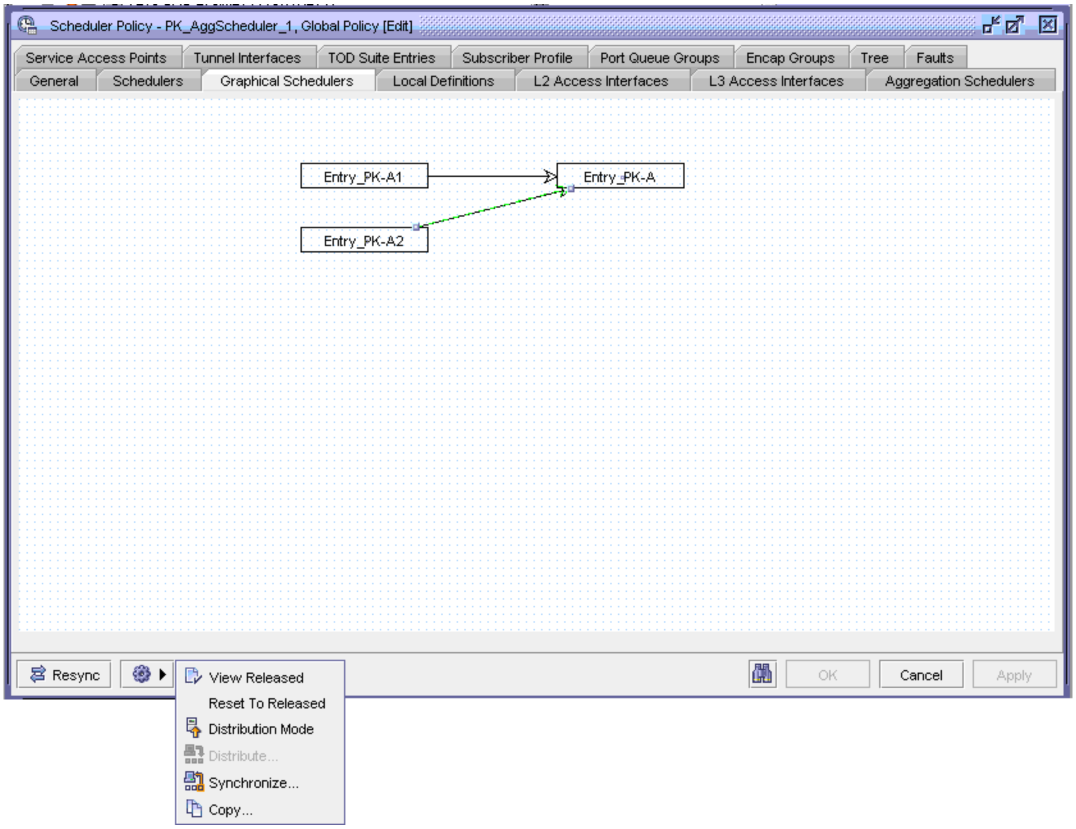
8 Click on the OK button. The Entry, Scheduler Policy (Create) form closes and a dialog box appears.

9 Click on the OK button. The newly configured scheduler is added to the list of schedulers.

10 To add additional schedulers to the policy, repeat steps 6 to 9.

11 Click on the Graphical Schedulers tab button to view a graphical display of the scheduler hierarchy within the scheduler policy. An example of the graphical display is shown in Figure 47-6.

Figure 47-6 Scheduler Policy form - Graphical Schedulers



12 Click on the Apply button.

13 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

14 Close the Scheduler Policy form. The Manage Scheduler Policies form reappears.

15 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-16 To configure an HSMDA scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler from the 5620 SAM main menu. The Manage HSMDA Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Rate (Mbps)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Group Rates tab button.

5 Configure the Rate (Mbps) parameter for group 1 and group 2.

6 Click on the HSMDA Scheduler Classes tab button.

7 Configure the parameters for classes 1 to 8:

- Group
- Weight
- Rate (Mbps)

The Group parameter must be configured with the same group (Group 1 or Group 2) for up to three sequential classes for each group. For example, when you configure Class 1 as Group 2, you can configure Class 2 and Class 3 as Group 2, but not as Group 1.

The Rate (Mbps) parameter is configurable when the Group parameter is set to None. The Weight parameter is configurable when the Group parameter is set to a value other than None.

8 Click on the Apply button.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the Scheduler Policy form. The Manage Scheduler Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 47-17 To configure an HSMDA WRR Policy

The HSMDA WRR Policy is only applicable to the 7750 SR-7 and -12, NE release 9.0 R3 and later.

1 Choose Policies→QoS→SROS QoS→Scheduler→HSMDA WRR Policy from the 5620 SAM main menu. The Manage HSMDA WRR Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA WRR Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Include Queues
- Schedule Using Class
- Weight

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The Global Policy Configuration block appears on the form.

5 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. The Distribute HSMDA WRR Policy form opens.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

6 Select the devices you want to distribute the policy to from the list of Available Nodes and click the right-pointing arrow to move the devices into the Selected Nodes list.

7 Click the Distribute button.

When the Policy has been successfully distributed, the selected devices will appear on the list under the Local Definitions tab button.

8 Policy parameters for a specific local device can be modified by selecting the device from the Local Definitions list and clicking on Properties. The HSMDA WRR Policy (Edit) form for the device opens. Any changes you make here will only affect the selected device.

9 Close the HSMDA WRR Policy form. The Manage HSMDA WRR Policies form reappears.

The newly created policy or policies appear in the bottom panel of the form.

10 For an existing HSMDA WRR policy, you can also determine which objects currently refer to the policy by checking the following tabs, selecting an item, and clicking the Properties button:

- L2 Access Interfaces
- L3 Access Interfaces
- Network Queue Policies
- Access Egress Policies
- Subscriber Profiles

11 Close the Manage HSMDA WRR Policies form.

Procedure 47-18 To configure a port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Port Scheduler from the 5620 SAM main menu. The Manage Port Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Rate (kbps)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

The Maximum Rate (kbps) parameter is configurable when the MAX check box is deselected.

4 Click on the Groups tab button.

5 Click on the Create button. The Port Scheduler Group (Create) form opens.

6 Configure the parameters:

- Displayed Name
- PIR (kbps)
- CIR (kbps)

The PIR (kbps) and CIR (kbps) parameters are configurable when the associated MAX check box is deselected.

7 Click on the Apply button. A dialog box appears.

8 Click on the OK button. The Port Scheduler Group (Create) form closes and the Port Scheduler (Create) form reappears.

9 Click on the Level tab button.

10 Click on the Select button in any of the Level panels to choose a port scheduler group from the list in the Select Group form. The port scheduler group must be preexisting on the port scheduler policy (see step 4).

11 Configure the parameters:

- PIR (kbps) (level 1)
- CIR (kbps) (level 1)
- Weight in group (level 1)
- PIR (kbps) (level 2)
- CIR (kbps) (level 2)
- Weight in group (level 2)
- PIR (kbps) (level 3)
- CIR (kbps) (level 3)
- Weight in group (level 3)
- PIR (kbps) (level 4)
- CIR (kbps) (level 4)
- Weight in group (level 4)
- PIR (kbps) (level 5)
- CIR (kbps) (level 5)
- Weight in group (level 5)
- PIR (kbps) (level 6)
- CIR (kbps) (level 6)
- Weight in group (level 6)
- PIR (kbps) (level 7)
- CIR (kbps) (level 7)
- Weight in group (level 7)
- PIR (kbps) (level 8)
- CIR (kbps) (level 8)
- Weight in group (level 8)
- Level
- Weight
- CIR Level
- CIR Weight

Note — Contiguous mapping of levels to a group is enforced. Priority levels cannot be added to a group unless the resulting set of priority levels is contiguous. When a level is not explicitly mapped to any group, it maps directly to the root of the port scheduler at its own priority.

The PIR (kbps) to PIR (kbps) and CIR (kbps) to CIR (kbps) parameters are each configurable when the associated MAX check box is deselected.

The Weight in group to Weight in group parameters are configurable when a port scheduler group is associated with the port scheduler policy.

12 Click on the Apply button.

13 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

14 Close the Port Scheduler Policy configuration form. The Manage Port Scheduler Policies form reappears.

15 Close the Manage Port Scheduler Policies form.

Procedure 47-19 To configure a 7210 SAS port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→7210 Port Scheduler from the 5620 SAM main menu. The Manage 7210 Port Scheduler Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

   b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Mode

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 If you selected a value of WeightedRoundRobin or WeightedDeficitRoundRobin for the Mode parameter, go to step 5. Otherwise go to step 7.

5 Click on the Queues tab button.

6 Configure the Weight parameter for queues 1 to 8.

7 Click on the Apply button.

8 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

9 Close the Port Scheduler form. The Manage 7210 Port Scheduler Policies form reappears.

Procedure 47-20 To configure a policer control policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Policer Control from the 5620 SAM main menu. The Manage Policer Control Policies form opens.

2 Perform one of the following steps.

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Policer Control Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Arbiter tab button.

i Click on the Create button. The Arbiter (Create) form opens.

ii Configure the parameters:

- Arbiter Name
- Description
- Tier
- Priority Level
- Weight
- Frame Based Bandwidth Rate
- Parent Arbiter
  The Parent Arbiter parameter is configurable when the Tier parameter is set to 2.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Arbiter (Create) form closes, and the Policer Control Policy form reappears.

5 (Optional step) Click on the Graphical Arbiters tab button to view a graphical display of the arbiter hierarchy within the policer control policy. You can perform any of the following steps.

a Right-click on the grid and select New Arbiter from the drop-down menu. The Arbiter (Create) form opens. You can create a new arbiter, as described in step 4.

b Right-click on an arbiter object and select Edit from the drop-down menu. The Arbiter (Edit) form opens. You can change the arbiter, as described in step 4.

c Right-click on an arbiter and select Remove from the drop-down menu. The arbiter object is removed from the hierarchy.

d Click on a Tier 2 arbiter object and draw a line to a Tier 1 arbiter object. The Tier 1 arbiter becomes the parent of the Tier 2 arbiter.

6 Click on the Tree tab button to view a hierarchical display of the policer control policy properties and sub components.

7 Click on the Priority Level tab button to configure the MBS contribution for eight priority levels. For each level, configure the following parameters:

- Cumulative MBS Contribution
- Fixed MBS contribution

8 Click on the Apply button.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the network elements. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the Policer Control form. The Manage Policer Control Policies form reappears.

Procedure 47-21 To configure a named buffer pool policy

To associate a Named Buffer Pool to a MDA, see Procedure 19-24.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Manage Named Buffer Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Weight
- MDA Weight
- Port Weight

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To configure Q1 pools perform steps 3 to 10 in Procedure 47-28.

5 Click on the Apply button.

6 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

7 Close the Named Pool Policy form. The Manage Named Buffer Pool Policies form reappears.

8 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

9 Close the Manage Named Buffer Pool Policies form.

Procedure 47-22 To configure an ingress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Ingress Template from the 5620 SAM main menu. The Manage Ingress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Queues tab button.

5 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- ID
- Displayed Name
- Description
- Multipoint
- Mode
- Policed
- Expedite

7 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.

Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 47-21.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

8 Configure the Scheduler button parameter.

i Click on the Select button beside the Scheduler button parameter. The Schedulers form opens.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

9 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab button.

ii Configure the parameters:

- CIR (kbps)
- PIR (kbps)
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

10 Configure the Burst Size parameters.

i Click on the Burst Size tab button.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

iii Click on the OK button. A dialog box appears.

11 Close the Ingress Queue Group Template Policy form.

Procedure 47-23 To configure an egress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Egress Template from the 5620 SAM main menu. The Manage Egress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Queues tab button.

5 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- ID
- Displayed Name
- Description
- Port Parent
- Rate Type
- Expedite
- Level
- Weight
- CIR Level
- CIR Weight

The Level, Weight, CIR Level, and CIR Weight parameters are configurable only if the Port Parent parameter is set to True.

7 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.

Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 47-21.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

8 Configure the Scheduler button parameter.

i Click on the Select button beside the Scheduler button parameter. The Schedulers form opens.

Note — The Scheduler parameter is configurable only if you set the Port Parent parameter to False.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

9 Configure the WRED Queue parameters.

i Select the Use WRED Queue parameter.

ii Click on the Select button beside the Displayed Name parameter. The Select WRED Queue Slope Policy form opens.

Note — Before you can select a WRED Queue Slope policy, you must create the policy using Procedure 47-8.

iii Specify a filter to search for existing policy.

iv Select the WRED Slope policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

10 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab button.

ii Configure the parameters:

The choice of CIP and PIR parameter definitions depends on the Rate Type parameter setting on the General tab.

- CIR (kbps) - if Rate Type parameter is set to Specific
- PIR (kbps) - if Rate Type parameter is set to Specific
- CIR (Percentage) - if Rate Type parameter is set to Percentage
- PIR (Percentage) - if Rate Type parameter is set to Percentage
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

11 Configure the Burst Size parameters.

i Click on the Burst Size tab button.

ii Configure the parameters:

- Committed Burst Size (kb)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit (kb)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (kb) value is lower than the Maximum Burst Size (bytes) value.

iii Click on the OK button. A dialog box appears.

iv Click on OK.

12 Click on the Forwarding Classes tab button.

13 Perform one of the following:

a Specify a filter to search for and edit an existing forwarding class. Use the filters to search for and open an existing forwarding class by choosing a forwarding class in the filtered list and clicking on the Properties button.

b Click on the Create button. The Forwarding Class (Create) form opens.

14 Configure the parameters:

- Forwarding Class
- Queue ID

15 Close the Egress Queue Group Template Policy form.

Procedure 47-24 To configure a 7705 SAR fabric profile

1 Choose Policies→QoS→SROS QoS→7705 SAR Fabric from the 5620 SAM main menu. The Manage Fabric Profiles form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 7705 SAR Fabric Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Mode

4 Click on the Rates tab button. In Aggregate mode, one rate is displayed. In Destination mode, six rates are displayed. Perform one of the following:

a For Aggregate mode, configure the Aggregate Rate parameter to set the fabric shaping rate to the daughter card slots.

b For Destination mode, configure the Rate To MDA (destRateTo1<card#> parameter for each daughter card slot to set the fabric shaping rate to each daughter card.

You can also configure the MultiPoint Rate parameter to be distributed to all of the daughter cards.

5 Click on the Apply button. The form changes to enable the other tabs.

6 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

7 Close the 7705 SAR Fabric form. The Manage 7705 SAR Fabric form is updated.

8 Click on the Search button to display the newly created profile or profiles in the bottom panel of the form.

9 Close the Manage 7705 SAR Fabric form.

Procedure 47-25 To configure a 7210 SAS remarking policy

The 7210 SAS remarking policy is used to configure the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces. A 7210 SAS remarking policy can be associated with the following 7210 SAS QoS policies:

- Port Access Egress Policy (the remarking policy must be DOT1P or DOT1P-LSP-EXP SHARED)
- Network Policy (the remarking policy must be LSP-EXP or DOT1P-LSP-EXP SHARED)
- Network Queue Policy (the remarking policy must be DOT1P-DSCP, DOT1P, or DSCP)

1 Choose Policies→QoS→SROS QoS→7210 Remarking from the 5620 SAM main menu. The Manage Remarking Policies form opens.

2 Perform one of the following:

  a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

  b Click on the Create button. The 7210 Remarking Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Type

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The 7210 Remarking Policy (Edit) form appears with the General tab displayed.

5 Click on the Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 47-1, are displayed on the form. Configure the forwarding class parameters, as required.

6 Double-click on a forwarding class. The 7210 Remark Forwarding Class (Edit) form opens.

7 Configure the parameters:

- Dot1P-LSP-EXP-Shared In Profile
- Dot1P-LSP-EXP-Shared Out Profile

8 Click on the OK button. The 7210 Remark Forwarding Class (Edit) form closes and the 7210 Remarking Policy (Edit) form appears.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The 7210 Remarking Policy (Edit) form closes and the Manage Remarking Policies form appears.

11 Click on the Search button to display a list of 7210 remarking policies.

12 Choose a 7210 remarking policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 46 for more information.

Procedure 47-26 To configure a 7210 MPLS LSP-Exp Map policy

Use this procedure primarily for RSVP LSP with FRR one-to-one. For LDP LSPs, or when using FRR facility, use of a single MPLS LSP-Exp Map policy for all IP interfaces is recommended. Local LDP FC Enable needs to be set to true from CLI.

1 Choose Policies→QoS→SROS QoS→7210 MPLS LSP-Exp Map from the 5620 SAM main menu. The 7210 MPLS LSP-Exp Map Policies form opens.

2 Click on the Create button. The 7210 MPLS LSP-Exp Map Policy (Create) form opens with the general tab displayed.

3 Configure the parameters:

- Policy Id
- Auto-Assign ID
- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the MPLS LSP-Exp Bits tab button.

5 Select a bit from the list and click on the Properties button. The MPLS LSP-Exp Map Profile (Create) form opens.

6 Configure the Profile parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The MPLS LSP-Exp Map Profile (Create) form closes.

9 Repeat steps 5 to 8 as required.

10 Click on the OK button. The 7210 MPLS LSP-Exp Map Policy (Create) form closes.

Procedure 47-27 To configure an HSMDA pool policy

To associate an HSMDA buffer pool with an MDA, see Procedure 19-24.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool from the 5620 SAM main menu. The Manage HSMDA Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- System Reserve (%)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Root Pools tab button.

5 Configure the Allocation Weight parameter for root pools 1 to 8.

The Allocation Weight parameter is configurable when the Default check box is deselected.

6 Click on the Class Pools tab button.

7 Configure the parameters for root pools 1 to 8:

- Root Parent
- Allocation Percent

The Allocation Percent parameter is configurable when the Default check box is deselected.

8 Click on the Apply button.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the HSMDA Pool Policy form. The Manage HSMDA Pool Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

12 Close the Manage HSMDA Pool Policies form.

Procedure 47-28 To configure Q1 pools

You must configure a Q1 pool to before you can assign the pool to an access ingress, access egress, network queue or shared queue policy.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Manage Named Buffer Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Click on Q1 Pool tab button. A list of configured Q1 Pools is displayed.

4 Perform one of the following steps:

a Select an existing Q1 pool. A QI Pool (Edit) form opens with the General tab displayed. Go to step 5.

b Click on the Create button. A Q1 Pool (Create) form opens with the General tab displayed. Go to step 5.

5 Configure the parameters:

- Pool Name
- Description
- Network Weight
- Access Weight

6 Click on the Select button beside the Displayed Name parameter. The Select Slope Policy - Q1 Pool list form opens.

7 Select a policy in the list and click on the OK button. The Select Slope Policy - Q1 Pool list form closes and the Q1 Pool (Create) form is refreshed with the slope policy information.

8 Configure the remaining parameters:

- Reserved CBS (%)
- Default Reserved CBS
- Amber Alarm Action Max (%)
- Amber Alarm Action Step (%)
- Amber Alarm Threshold (%)
- Red Alarm Threshold (%)

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Q1 Pool configuration form closes and the Named Pool Policy form reappears.

11 Click on the Ok button. A dialog box appears.

12 Click on the OK button. The Named Pool Policy configuration form closes and the Manage Named Buffer Pool Policies form reappears.

13 Close the Manage Named Buffer Pool Policies form.

Procedure 47-29 To create an aggregation scheduler

You can create an aggregation scheduler when you have created two or more scheduler policies. See "Hierarchical schedulers" in this chapter for more information.

1 Create two or more scheduler policies, as described in Procedure 47-15.

2 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

3 Specify a filter to search for an existing customer and click on the Search button.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Sites tab button.

6 Select a site in the list and click on the Properties button. The Site (Edit) form opens.

7 Click on the Aggregation tab button.

8 Click on the Create button. The Create Aggregation Scheduler wizard opens.

9 Select a site in the list and click on the Next button.

10 Configure the parameters:

- Scheduler Name
- Description

11 Click on the Next button. The Select Assignment Scope step is displayed.

12 Configure the Equipment Type parameter.

13 Click on the Next button. The Select Card or the Select Port step is displayed, depending on the option chosen for the Equipment Type parameter.

14 Click on the Select button to specify a card or port. The Select Card - Aggregation Scheduler form or the Select Port - Aggregation Scheduler form opens.

15 Select a card or port in the list and click on the OK button. The Select - Aggregation Scheduler form closes and the card or port information is displayed on the Select Card or Select Port form.

16 Click on the Next button. The Select Ingress and Egress Scheduler Policies step is displayed.

17 Click on the Select buttons to choose ingress and egress scheduler policies. The Select Policy - Aggregation Scheduler form opens.

18 Set the filter criteria, if required, and click on the Search button. A list of policies is displayed.

19 Select a policy in the list and click on the OK button. The Select Policy - Aggregation Scheduler form closes and the policy information is displayed in the Select Ingress and Egress Scheduler Policies form.

20 If you are creating an aggregation scheduler for an IOM3 port, then go to step 21. Otherwise go to step 25.

21 Click on the Next button. The Select Ingress and Egress Policer Control Policies step is displayed.

22 Click on the Select buttons to choose ingress and egress policer control policies. The Select Policer Control Policy - Aggregation Scheduler form opens.

23 Set the filter criteria, if required, and click on the Search button. A list of policies is displayed.

24 Select a policy in the list and click on the OK button. The Select Policer Control Policy - Aggregation Scheduler form closes and the policy information is displayed in the Select Ingress and Egress Policer Control Policies form.

25 Click on the Next button. The Select Time Of Day Suite Policy step is displayed.

26 Click on the Select button to choose a time of day suite. The Select Time Of Day Suite - Aggregation Scheduler form opens.

27 Select a time of day suite entry and click on the OK button. The Select Time Of Day Suite - Aggregation Scheduler form closes and the policy information is displayed in the Select Time Of Day Suite Policy form.

28 Click on the Finish button. A dialog box appears.

29 Click on the OK button. The aggregation scheduler is listed in the Aggregation tab of the Site (Edit) form.

30 Close the Site (Edit) form. The Customer (Edit) form reappears.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The Customer (Edit) form closes and the Manage Customers form reappears.

33 Close the Manage Customers form.

Procedure 47-30 To configure an ANCP MSS static map

You can configure an ANCP MSS static map when you have created an ANCP policy and an aggregation scheduler.

1 Create an ANCP policy, as described in Procedure 68-2.

2 Create an aggregation scheduler, as described in Procedure 47-29.

3 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Aggregation tab button.

6 Select a site in the list and click on the Properties button. The Aggregation Scheduler (Edit) form opens.

7 Click on the ANCP Static Map button.

8 Select an ANCP policy in the list and click on the Create button. The ANCP MSS Static Map (Create) form opens.

9 Configure the parameters:

- ANCP String
- Displayed Name

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ANCP Policy is listed in the ANCP Static Map tab of the Aggregation Scheduler (Edit) form.

12 Click on the OK button to close the Aggregation Scheduler (Edit) form. The Customer (Edit) form reappears.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button.

15 Close the Manage Customers form.

Procedure 47-31 To configure an ATM QoS policy

1 Choose Policies→QoS→SROS QoS→ATM QoS from the 5620 SAM main menu. The Manage ATM QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The ATM QoS Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name
- Description

4 Click on the QoS tab button.

5 Configure the parameters:

- Service Category
- MIR (kbps)
- PIR (kbps)
- CDVT
- Shaping
- Policing
- Descriptor Type
- CLP Tagging

6 Click on the OK button to save the policy. The ATM QoS Policy (Create) form closes and the Manage ATM QoS Policies form reappears.

7 Click on the Search button to display the newly created policy or policies.

8 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

9 Close the Manage ATM QoS Policies form.

Procedure 47-32 To configure a 9500 MPR ATM QoS policy

1 Choose Policies→QoS→9500 MPR QoS→ 9500 ATM QoS from the 5620 SAM main menu. The 9500 ATM QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 9500 ATM QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name

4 Click on the QoS tab button.

5 Configure the parameters:

- Service Category
- Policing
- PCR (cells/second)
- CDVT (microseconds)
- MDCR

6 Click on the OK button to save the policy. The ATM QoS Policy (Create) form closes and the 9500 ATM QoS Policies form reappears.

7 Click on the Search button to display the newly created policy or policies.

8 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

9 Close the 9500 ATM QoS Policies form.

Procedure 47-33 To configure and distribute a 9500 Radio Interface Queue Map policy

When configuring a 9500 Radio Interface Queue Map policy, the following QoS variants are supported: ODU, MPT-HL, MPT-HC/MPT-MC.

1 Choose Policies→QoS→9500 MPR QoS→ 9500 Radio Interface Queue Map from the 5620 SAM main menu. The 9500 Radio Interface Map Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for a policy. Choose a policy from the list, modify the policy and click on the Properties button.

   b Click on the Create button. The 9500 Radio Interface Queue Map Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Description

4 Click on the Radio Interface Queue Map tab button.

5 Perform one of the following:

   a Specify a filter to search for a policy. Choose a policy from the list, modify the policy and click on the Properties button.

   b Click on the Create button. The 9500 Radio Interface Queue Map Global Policy (Create) form opens.

6 Configure the parameters in the Radio Interface and Queue Size Settings panel:

- Card ID
- Port ID
- Snmp Port ID
- Status
- Reset all Queues
- Queue 1 Size
- Queue 2 Size
- Queue 3 Size
- Queue 4 Size
- Queue 5 Size

Note — You cannot configure the queue size parameters when the Reset all Queues parameter is selected.

7 Click on the OK or Apply button to apply the changes and return to the 9500 Radio Interface Queue Map Global Policy (Create) form. The newly created policy is displayed.

8 Select the newly created policy, and choose the Properties button. The 9500 Radio Interface Queue Map Global Policy (Edit) form opens with the General tab displayed.

9 Click on the Switch Mode button beside the Configuration Mode parameter to distribute the policy.

10 Choose a policy in the list from the 9500 Radio Interface Map Policies form and perform one of the following:

a Click on the Distribute button in the 9500 Radio Interface Map Policies form. See Procedure 46-1 for more information about how to release and distribute the newly created or modified policy.

b Click on the Properties button, the 9500 Radio Interface Queue Map Global Policy (Edit) form is displayed. Click on the More Actions button and choose Distribute from the drop-down to distribute the policy locally to devices. See Procedure 46-1 for more information about how to release and distribute the newly created or modified policy. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

11 Close the 9500 Radio Interface Map Policies form.

Procedure 47-34 To configure and distribute a 9500 NE QoS policy

1 Choose Policies→QoS→9500 MPR QoS→ 9500 NE QoS from the 5620 SAM main menu. The 9500 NE QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for a policy. Choose a policy from the list, modify the policy and click on the Properties button.

b Click on the Create button. The 9500 NE QOS Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- QoS Classification
- Description

For the QoS Classification parameter, choose one of the following:

a 802.1p and click on the Dot1p tab button

b DiffServ and click on the DSCP tab button

4 Click on the QueueMap policy tab button and choose Select. The Select 9500 Radio Interface Queue Map Policy form is displayed.

Note — You can link the Interface Queue Map policy as described in Procedure 47-33 to the NE Qos Policy.

5 Choose a policy and click on the OK button. The 9500 NE QOS Global Policy (Create) form opens.

6 Click on the Global Queue Setting tab button. To change the algorithm, choose an algorithm and choose Properties. The RadioQ (Multiple Instances) (Edit) form is displayed.

7 Configure the parameters:

- Queue Number
- Algorithm
- Weight

8 Click on the OK button to open the 9500 NE QoS Policies form. The newly created policy is displayed.

9 Select the newly created policy, and choose the Properties button. The 9500NE QOS Global Policy (Edit) form opens with the General tab displayed.

10 Click on the Switch Mode button beside the Configuration Mode parameter to distribute the policy. See Procedure 46-1 for more information on how to release and distribute the newly created policy.

11 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Close the 9500 NE QoS Policies form.

Procedure 47-35 To configure a 7250 SAS or Telco QoS level policy

1 Choose Policies→QoS→7250 SAS and Telco QoS from the 5620 SAM main menu. The Manage 7250 SAS and Telco QoS Node Level Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco Qos Node Level Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name
- Description
- Queue Algorithm

4 If the Queue Algorithm parameter is set to Strict Priority, go to step 6.

5 Click on the Scheduling Tx Queue tab button.

i Configure the Txq 0 to Txq 7 parameters, depending on the number of queues. There is one Txq parameter for each queue. The number of queues and Txq parameters depends on the Queue Algorithm parameter value chosen in step 3.

ii Repeat step i for each Txq parameter on the Scheduling Tx Queue tab.

6 Click on the Traffic Class Entries tab button.

7 Click on the Create button. The QoSTrafficClassEntry (Create) form opens.

8 Configure the parameters:

- Traffic Class
- DSCP
- Priority
- Color
- DSCP Value

The DSCP Value parameter is configurable when the DSCP parameter is enabled.

9 To add more policy entries, repeat steps 7 to 8.

10 Click on the OK button. The QoSTrafficClassEntry (Create) form closes and the Manage 7250 SAS and Telco QoS Node Level Policies form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

13 Close the Manage 7250 SAS and Telco QoS Node Level Policies form.

Procedure 47-36 To configure an OmniSwitch QoS policy condition

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing condition. Select a condition in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Condition. The AOS QoS Condition, Global Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Filter Properties tab button. The Filter Properties form opens with the Port tab displayed.

5 Configure the parameters in the Port Match Criteria panel, if required:

- Match Source Port
- Source Slot
- Source Port
- Match Destination Port
- Destination Slot
- Destination Port

6 Click on the Layer 2 tab button.

7 Configure the parameters in the MAC Match Criteria panel, if required:

- Source MAC
- Source Mask
- Destination MAC
- Destination Mask

8 Configure the Source VLAN parameter in the Source VLAN Match Criteria panel, if required.

9 Configure the Priority parameter in the 802.1p Match Criteria panel, if required.

10 Click on the Layer 3 tab button.

11 Configure the parameters in the IP Match Criteria panel:

- Source IP
- Source Mask
- Source Net Mask
- Destination IP
- Destination Mask
- Destination Net Mask
- VRF Status
- VRF Name

12 Configure the parameters in the DSCP Match Criteria panel, if required:

- Differentiated Services Code Point
- Mask

13 Configure the parameters in the ToS Match Criteria panel, if required:

- ToS Precedence
- Mask

14 Configure the parameters in the ICMP Match Criteria panel, if required:

- ICMP Code
- ICMP Type

15 Click on the Layer 4 tab button.

16 Configure the IP Protocol parameter.

The following parameters are not displayed when the IP Protocol parameter is set to HOPOPT.

17 Configure the parameters in the IP Port Match Criteria panel, if required:

- Match Source IP Port Range
- Source IP Port (Start)
- Source IP Port (End)
- Match Destination IP Port Range
- Destination IP Port (Start)
- Destination IP Port (End)

18 Click on the OK button. The AOS QoS Condition, Global Policy (Create) form closes.

19 To create more QoS policy conditions, repeat steps 2b to 18.

20 Close the AOS QoS Policies form.

Procedure 47-37 To configure an OmniSwitch QoS policy action

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing action. Select an action in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Action. The AOS QoS Action, Global Policy (Create) form opens with the General tab displayed.

Note — You cannot use DSCP and ToS parameters in the same action.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the Action parameter in the Disposition panel.

5 Configure the parameters in the Priority and Bandwidth panel:

- Priority
- Maximum Bandwidth (Kbps)
- Share Resources

6 Configure the Priority parameter in the 802.1p panel.

7 Configure the Differentiated Services Code Point parameter in the DSCP panel.

8 Configure the Type of Service parameter in the ToS panel.

9 Configure the parameters in the Redirect panel, if required.

- Slot
- Port
- LAG Number

10 Click on the OK button. The AOS QoS Action, Global Policy (Create) form closes.

11 To create more actions, repeat steps 2b to 10.

12 Close the AOS QoS Policies form.

Procedure 47-38 To create an OmniSwitch QoS policy

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Policy. The AOS QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Policy Status
- Precedence

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Action panel to choose an action for the policy. The Select Action - QoS Policy form opens with a list of available actions displayed.

5 Select an action and click the OK button. The Select Action - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

6 Click on the Select button in the Condition panel to choose a condition for the policy. The Select Action - QoS Policy form opens with a list of available conditions displayed.

7 Select a condition and click the OK button. The Select Condition - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

8 To create more policies, repeat steps 2b to 9.

9 Click on the OK button. The AOS QoS Policy, Global Policy (Create) form closes and the AoS QoS Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Close the AOS QoS Policies form.

Procedure 47-39 To create an OmniSwitch QoS list

This procedure is used to configure a QoS list, which is a collection of QoS polices. This QOS list includes support of egress policy configurations to perform last minute operations on the data traffic before it egresses through the port.

See Procedures 47-36, 47-37, and 47-38 to create AOS QoS policy actions, policy conditions, and policies.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Click on the Create button and choose Create QoS List. The AOS QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Displayed Name
- List Type
- Policy Status

Note — Do not use a colon to create the displayed name because the 5620 SAM uses colons as separators for the object full name.

4 To add an AOS QoS policy to the QoS list, click on the List Policies tab button.

5 Click on the Create button. The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form opens.

6 Click on the Select button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form opens.

7 Select a policy entry. Click on the OK button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form closes.

8 The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form reappears, with the policy name selected in Step 7 displayed in the Displayed Name field.

9 Click on the Properties button. The AOS QoS Policy -<policy name>, Global Policy (Edit) form opens.

10 If required, configure the Precedence parameter.

11 Close the AOS QoS Policy -<policy name>, Global Policy (Edit) form

12 The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form reappears. Click on the OK button. A dialog box appears.

13 Click on the OK button.

14 Close the AOS QoS Policy, Global Policy (Create) form.

Procedure 47-40 To create or configure a MC MLPPP ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MLPPP Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MlpppIngressQosProfileClass (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policy or policies in the bottom panel of the form.

13 Close the Manage MLPPP Ingress QoS Profile form.

Procedure 47-41 To create or configure a MC MLPPP egress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default egress MC profiles, but you cannot delete them.

b Click on the Create button. The MLPPP Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MlpppEgressQosProfileClass (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the Forwarding Classes tab button.

11 Select a forwarding class in the list and click on the Properties button. The MlpppEgressQosProfileForwardingClass (Edit) form opens.

12 Configure the MLPPP Class parameter.

13 Click on the OK button to save the values and close the form.

14 Repeat steps 11 to 13 for each forwarding class that you need to configure.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

17 Click on the Search button to display any newly created policies in the bottom panel of the form.

18 Close the Manage MLPPP Egress QoS Profile form.

Procedure 47-42 To create or configure an MCFR ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Ingress QoS Profile from the 5620 SAM main menu. The Manage MCFR Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MCFR Ingress QoS Profile Class (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Ingress QoS Profile form.

Procedure 47-43 To create or configure an MCFR egress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Egress QoS Profile from the 5620 SAM main menu. The Manage MCFR Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default egress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MCFR Egress QoS Profile Class (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Egress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Egress QoS Profile form.

Procedure 47-44 To configure QoS policy overrides on an L2 or L3 access interface

Use this procedure to override some or all settings associated with an access ingress, access egress, or scheduler policy on an L2 or L3 access interface configured for a service.

See the following procedures for information about overriding access ingress, access egress, or scheduler policies that are associated with residential subscribers:

- Procedure 68-13 for the overrides associated with SLA profiles
- Procedure 68-14 for the overrides associated with subscriber profiles

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with Service (Service Management) selected in the filter list.

2 Choose Access Interface (Service Management) from the object drop-down list.

3 Click on one of the following icons listed below the Access Interface (Service Management) icon.

- L2 Access Interface (Service Management)
- L3 Access Interface (Service Management)

4 Set the filter criteria, if required, and click on the Search button. A list of L2 or L3 access interfaces is displayed.

5 Select an interface in the list and click on the Properties button. Based on the interface that you chose in step 3, the L2 Access Interface form or L3 Access Interface form opens.

6 Perform one of the following:

a Create an override for an access ingress or access egress policy queue. Go to step 7.

b Create an override for an access egress policy HSMDA queue. Go to step 15.

c Create an override for an ingress or egress policy policer. Go to step 25.

d Create an override for an ingress or egress policer control policy. Go to step 34.

e Create an override for an ingress or egress scheduler policy. Go to step 46.

7 Click on the Override Policy Items tab button. Perform one of the following actions.

a Click on the Access Ingress Queues tab button.

b Click on the Access Egress Queues tab button.

8 Click on the Create button.

Based on the tab that you selected in step 7, the Access Ingress Queue Override form or the Access Egress Queue Override form opens with the General tab displayed.

9 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue form opens.

ii Choose the policy queue.

iii Click on the OK button. The queue override form reappears with the configured values for the policy queue.

10 Click on the Override tab button.

11 Configure the parameters, as required:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override High Priority Reserved
- Override PIR Adaptation
- Override CIR Adaptation
- Override Queue Weight
- Override Queue CIR Weight
- Override Port Average Overhead

Overrides for the PIR and CIR are configured in kbps if the Rate Type for the queue was originally set to kbps. The PIR and CIR overrides are configured as a percentage (%) if the Rate Type for the queue was originally set to either Percent Port Limit or Percent Local Limit.

The Override Port Average Overhead parameter is only configurable for access egress queues.

To override any of these parameters, you must select the appropriate check box. Deselect the associated Default or MAX check box to enter a specific value, or to select a drop-down parameter option.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The queue override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

14 Go to step 55.

15 Click on the Override Policy Items tab button.

16 Click on the Access Egress HSMDA Queues tab button.

17 Click on the Create button.

The Access Egress HSMDA Queue Override form opens with the General tab displayed.

18 Choose the queue that you want to override.

i Click on the Select button. The Select Access Egress Policy Queue form opens.

ii Choose the queue.

iii Click on the OK button. The Access Egress HSMDA Queue Override form reappears with the configured values for the queue.

19 Click on the Override tab button.

20 Configure the parameters:

- PIR (kbps)
- Maximum Burst Size (bytes)
- WRR Weight

If you select the Override check box for a parameter, the original parameter value is displayed.

To specific another override value for the PIR (kbps) parameter, you must first deselect the associated MAX check box. To specific another override value for the Maximum Burst Size (bytes) parameter you must first deselect the associated Default check box.

You can only specify an override value for WRR Weight for queues 1, 2, or 3.

21 Choose the HSMDA Slope policy that you want to override.

i Click on the Select button. The Select HSMDA Slope Policy form opens.

ii Select the policy.

iii Click on the OK button. The queue override form reappears with the selected HSMDA Slope policy name displayed.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The queue override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

24 Go to step 55.

25 Click on the Override Policy Items tab button. Perform one of the following actions.

a Click on the Ingress Policer tab button.

b Click on the Egress Policer tab button.

26 Click on the Create button. The policer override form opens.

27 Click on the Select button. The select policy policer form opens.

28 Select a policy policer and click on the OK button. The select policy policer form closes and the policer override form refreshes with the configured values for the policy policer.

Note — Policy policers must be applied to the L2 Access Interface or the L3 Access Interface in order to be selected.

29 Click on the Override tab button.

30 Select the Override check box for any of the following parameters, and then configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override Packet Offset
- Stats Mode

Overrides for the PIR and CIR are configured in kbps if the Rate Type for the policer was originally set to kbps. The PIR and CIR overrides are configured as a percentage if the Rate Type for the policer was originally set to Percent Local Limit.

To override any of these parameters, you must select the required check box. Deselect the associated Default or MAX check box to enter a specific value, or to select a drop-down parameter option.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

33 Go to step 55.

34 Click on the Override tab button. Perform one of the following actions.

a Click on the Ingress Policer Control tab button.

b Click on the Egress Policer Control tab button.

Note — Policer control policies must be applied to the L2 Access Interface or the L3 Access Interface in order to enable the policer control tab buttons.

35 Click on the Create button. The policer override form opens.

36 Select the Override check box for any of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

37 Click on the Level Override Policy Items tab button.

38 Select a Level Override from the list and click on the Properties button. The policy policer level override form opens with the General tab displayed.

39 Click on the Override tab button.

40 Select the Override check box, and then configure the Maximum Cumulative Buffer Space parameter.

41 Click on the OK button. A dialog box appears.

42 Click on the OK button. The policy policer level override form closes and the policer override form reappears.

43 Click on the OK button. A dialog box appears.

44 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

45 Go to step 55.

46 Click on the Schedulers tab button.

47 Choose the scheduler policy that you want to override.

i Click on the Select button to define the Ingress Scheduler and Egress Scheduler policy that you want to modify.

ii Choose the scheduler policy.

iii Click on the Apply button. A dialog box appears.

iv Click on the Yes button. The L2 Access Interface form or L3 Access Interface form reappears.

48 Click on the Override Policy Items tab button.

49 Perform one of the following actions.

a Modify the Ingress Scheduler parameters.

i Click on the Ingress Schedulers tab button.

ii Click on the Create button.

The Ingress policy scheduler override form opens with the General tab displayed.

b Modify the Egress Scheduler parameters.

i Click on the Egress Schedulers tab button.

ii Click on the Create button.

The Egress policy scheduler override form opens with the General tab displayed.

50 Choose the scheduler policy that you want to override.

i Click on the Select button. The Select Scheduler Policy Entry form opens.

ii Choose the policy entry.

iii Click on the OK button. The policy scheduler override form reappears with the configured values for the scheduler policy.

51 Click on the Override tab button.

52 Configure the parameters:

- Override Summed CIR
- Summed CIR
- Override PIR
- PIR (kbps)

53 Click on the OK button. A dialog box appears.

54 Click on the OK button. The scheduler entry override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

55 Click on the OK button to close the L2 Access Interface form or L3 Access Interface form.

48 — Filter policies

48.1 Filter policies overview

Filter policies specify a forward, drop, or HTTP redirect action for packets based on information specified as the match criteria. You can create up to 2000 IP and 2000 MAC filter policies per managed NE. You can create up to 131 071 entries in a filter policy.

Filter entry matching criteria are either general or specific, but all conditions must be met for the packet to be considered a match and the specified entry action performed. The process stops when the first complete match is found and the action defined in the entry is executed.

When an interface or circuit is not configured with a filter policy, all traffic is allowed. By default, there are no filters associated with services or interfaces.

The 5620 SAM supports the creation and management of the following filter policies:

- ACL IP filter policies—applied to network and access IP interfaces, and service tunnels
- ACL IPv6 filter policies—applied to access interfaces and service tunnels
- ACL MAC filter policies—applied to access interfaces and service tunnels
- ACL IGMP filter policies—applied to 7250 SAS and Telco interfaces

Note — The 7705 SAR does not support IPv6 and MAC ACL filters.

The 7705 SAR has the following configuration limits for ACL IP filter entries:

- For non-extended range filter entries, the match criteria cannot be defined to match more than 256 packets.
- For extended range filter entries, there is no limit on the number of packet matches for the defined criteria; however, the total number of unique match criteria in use across all extended range filter entries within the same ACL IP filter cannot exceed eight.

SAP and service tunnel forwarding

ACL IP and ACL MAC filters contain options for delivering packets to specific destination SAPs and service tunnels based on the match criteria. Because the forwarding action is specified separately from device configuration, the packet destination name must be entered directly in text form (for example, 1/1/2:500) and validated by the 5620 SAM. Consider the following before you create a SAP or service tunnel forwarding filter:

- Although you can configure them on other service types, you should only create these filters on a VPLS. On other service types, packets are dropped.
- You can apply these filters on an ingress, but not an egress, SAP or service tunnel.

- The destination SAP or service tunnel must be on the same service as the device on which the filter is applied.
- The encapsulation type of the destination SAP and the associated port must be the same. Supported encapsulations are Ethernet Null, dot1q, Q in Q, BCP, bridged Ethernet, FR, and ATM.

Web portal redirect

ACL IP and ACL MAC filters contain options for redirecting hosts to a URL address. The 7710 SR, 7750 SR-7, and 7750 SR-12 open a new connection to the specified web portal. The host can use the web portal to create or modify a service profile. The web portal updates the ACL policy directly, or through another system such as the 5750 SSC, to remove the redirection policy.

Note — The 7750 SR-1 does not support web portal redirect.

48.2 Filter policies procedures

The following procedures describe how to configure filter policies.

Procedure 48-1 To configure an ACL IP filter policy

1 Choose Policies→Filter→ACL IP Filter from the 5620 SAM main menu. The Manage ACL IP Filter Policies form opens.

2 Perform one of the following:

  a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

  The ACL IP Filter (Edit) form opens with the General tab displayed.

  b Click on the Create button.

  The ACL IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action

4 Click on the Insertion Blocks tab button.

5 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

6 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab button.

ii Click on the Create button. The Entry, ACL IP Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 6 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the Action parameter:

If you specify Forward, the Next Hop Routing tab appears. Perform the following:

- Click on the Next Hop Routing tab button.
- Configure the parameters:
    - Forward NH
    - Is Indirect
    - Forward NH Interface
    - Remark DSCP
    - Remark DSCP Mask
    - Remark Dot1p

If you specify forward (SAP), the Forwarding Destination tab appears. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
    - Port Name
    - Outer Encap Value
    - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is configurable. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
    - Path ID
    - VC ID

If you specify HTTP redirect, the Web Redirect tab appears. Perform the following:

- Click on the Web Redirect tab button.
- Configure the Redirect URL parameter.

viii Configure the parameters:

- Protocol
- DSCP
- Source IP
- Destination IP
- Src Mask
- Dst Mask
- Fragment
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option
- Source Port
- Dest Port
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack
- Source Route Option

The Source Port and Dest Port parameters are configurable only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is ICMP.

ix Click on the Cflowd tab button.

x Configure the parameters:

- Cflowd Sample
- Cflowd If Sample

xi Click on the OK button. The Entry, ACL IP Filter (Create) form closes and a dialog box appears.

xii Click on the OK button. The ACL IP Filter (Create) form reappears with the newly created filter entry displayed.

7 To create an additional filter entry, repeat step 6.

8 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. A dialog box appears.

v Click Yes to apply the change. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

9 Click on the OK button to save the policy. The ACL IP Filter form closes and the Manage ACL IP Filter Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select the newly created policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Select the distributed policy in the list and click on the Properties button. The ACL IP Filter Global Policy (Edit) form opens.

13 Click on the Local Definitions tab button.

14 Select a local definition from the list and click on the Properties button. The ACL IP Filter Local Policy (Edit) form opens.

15 Click on the Insertion Blocks tab button.

16 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

Note — The Group Entries Inserted panel displays the number of entries insterted on this filter range.

17 Configure the Application and Location parameters in the Group Insertion Sorting panel.

18 Click on the Sort Group Instertions button. A dialog box appears.

19 Click on the OK button.

20 Perform the following steps to view filter entry data.

i Click on the Filter Entries tab button.

ii Click on the Credit Control Entries tab button or the RADIUS Entries tab button.

iii Click on the Search button.

iv Select an entry from the list and click on the Properties button. A form opens.

v Close the form after viewing the filter entry data.

21 Close the ACL IP Filter Entry Local Policy (Edit) form.

22 Close the ACL IP Filter Entry Global Policy (Edit) form.

23 Close the Manage ACL IP Filter Policies form.

Procedure 48-2 To configure an ACL IPv6 filter policy

Note — The 7705 SAR does not support ACL IPv6 filters.

1 Choose Policies→Filter→ACL IPv6 Filter from the 5620 SAM main menu. The Manage ACL IPv6 Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button.

The ACL IPv6 Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action

4 Click on the Insertion Blocks tab button.

5 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

6 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab button.

ii Click on the Create button. The Entry, ACL IPv6 Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the ACL IPv6 filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 6 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Source Port
- Dest Port
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack

The Source Port and Dest Port parameters are configurable when the Protocol parameter value is TCP or UDP.

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is IPv6_ICMP.

viii Click on the OK button. The Entry, ACL IPv6 Filter (Create) form closes and a dialog box appears.

ix Click on the OK button. The ACL IPv6 Filter (Create) form displays the new filter entry.

7 To create an additional filter entry, repeat steps 6.

8 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

9 Click on the OK button. The ACL IPv6 Filter (Create) form closes, and the Manage ACL IPv6 Filter Policies form reappears.

10 Click on the Search button to display the newly created policy.

11 Select the policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Select the distributed policy in the list and click on the Properties button. The ACL IPv6 Filter Global Policy (Edit) form opens.

13 Click on the Local Definitions tab button.

14 Select a local definition from the list and click on the Properties button. The ACL IPv6 Filter Local Policy (Edit) form opens.

15 Click on the Insertion Blocks tab button.

16 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

Note — The Group Entries Inserted panel displays the number of entries insterted on this filter range.

17 Configure the Application and Location parameters in the Group Insertion Sorting panel.

18 Click on the Sort Group Instertions button. A dialog box appears.

19 Click on the OK button.

20 Perform the following steps to view filter entry data.

i Click on the Filter Entries tab button.

ii Click on the Credit Control Entries tab button or the RADIUS Entries tab button.

iii Click on the Search button.

iv Select an entry from the list and click on the Properties button. A form opens.

v Close the form after viewing the filter entry data.

21 Close the ACL IPv6 Filter Entry Local Policy (Edit) form.

22 Close the ACL IPv6 Filter Entry Global Policy (Edit) form.

23 Close the Manage ACL IPv6 Filter Policies form.

Procedure 48-3 To configure an ACL MAC filter policy

Note — ACL MAC filters are not supported for the 7705 SAR.

1 Choose Policies→Filter→ACL MAC Filter from the 5620 SAM main menu. The Manage ACL MAC Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The ACL MAC Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action
- MAC Filter Type

The Default Action parameter specifies the action to be applied to packets when no action is specified in the MAC filter entries or when the packets do not match the specified criteria.

4 Configure the filter entries. Perform the following:

i Click on the Filter Entries tab button.

ii Click on the Create button. The Entry, ACL MAC Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Auto-Assign ID
- Entry ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv Assign a time range to the ACL MAC filter entry by clicking on the Select button beside the Name parameter. The Select Time Range - MacFilterEntry list form opens.

v Select a time range entry and click on the OK button. The Select Time Range - MacFilterEntry list form closes and the Entry, ACL MAC Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the Action parameter:

If you specify forward (SAP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Port Name
  - Outer Encap Value
  - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Path ID
  - VC ID

If you specify HTTP redirect, the Web Redirect tab is displayed. Perform the following:

- Click on the Web Redirect tab button.
- Configure the Redirect URL parameter.

viii Click on the Filter Properties tab button.

ix Configure the parameters:

- Frame Type
- Source MAC
- Src Mask
- Destination MAC
- Dst Mask
- Dot1p
- Dot1p Mask
- Low ISID
- High ISID
- Inner Tag Value
- Inner Tag VID Mask
- Outer Tag Value
- Outer Tag VID Mask
- DSAP
- DSAP Mask
- SSAP
- SSAP Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Src Mask, Destination MAC, Dst Mask, Dot1p, Dot1p Mask, Low ISID and High ISID parameter pairs are configurable when the check box for each pair is selected.

The Low ISID and High ISID parameters are only configurable when the MAC Filter Type parameter is set to ISID.

The Inner Tag Value, Inner Tag VID Mask, Outer Tag Value, and Outer Tag VID Mask parameters are only configurable when the MAC Filter Type parameter is set to VID.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is set to e802dot2LLC and the MAC Filter Type parameter is set to Normal.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP and the MAC Filter Type parameter is set to Normal.

The Ether Type parameter is configurable only when the Frame Type parameter value is set to Ethernet II and the MAC Filter Type parameter is set to Normal.

x Click on the OK button. The Entry, ACL MAC Filter (Create) form closes and a dialog box appears.

xi Click on the OK button. The ACL MAC Filter (Create) form reappears with the newly created filter entry displayed.

5 By default, all IDs for filter entries are set to 0. Perform one of the following steps:

a Continue configuring the filter. Go to step 7.

b Reorder new or existing filter entries, using the New Entry ID parameter.

i Click on the Refresh button to find an existing filter entry. The list of filter entries is displayed.

ii Select a filter entry in the list.

iii Click on the Renumber ID button. The renumber entry ID form opens and displays the current filter ID.

iv Specify the New Entry ID parameter. The range is 1 to 65535.

v Click on the OK button. The renumber entry ID form closes and the list of filter entries is refreshed, based on the new ID number assigned to the filter.

6 To add an additional filter entry, repeat steps 4 and 5.

7 Click on the OK button to save the policy. The ACL MAC Filter (Create) form closes and the Manage ACL MAC Filter Policies form reappears.

8 Click on the Search button to display the newly created policy or policies.

9 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the Manage ACL MAC Filter Policies form.

Procedure 48-4 To configure a 7250 SAS and Telco ACL standard IP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL Standard IP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL Standard IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL Standard IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Create button. The 7250 SAS and Telco ACL Standard IP Filter entry form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Src Mask
- VLAN Priority Tag

The VLAN Priority Tag parameter is configurable when its check box is selected. The parameter is configurable by default.

9 To add more filter entries, repeat steps 5 to 8.

10 Click on the OK button. The 7250 SAS and Telco ACL Standard IP Filter entry form closes and the Manage 7250 SAS and Telco ACL Standard IP Filter Policies form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

13 Close the Manage 7250 SAS and Telco ACL Standard IP Filter Policies form.

Procedure 48-5 To configure a 7250 SAS and Telco ACL extended IP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL Extended IP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL Extended IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL Extended IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Create button. The 7250 SAS and Telco ACL Extended IP Filter entry form opens.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Destination IP
- Source Port
- Dest Port
- TCP Ack
- Protocol
- Src Mask
- Dest Mask
- TOS
- Precedence
- VLAN Priority Tag
- ICMP Code
- ICMP Type

The Source Port and Dest Port parameters are configurable when the Protocol parameter value is TCP or UDP.

The TCP Ack parameter is configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is ICMP.

9 To add more filter entries, repeat steps 5 to 8.

10 Click on the OK button. The 7250 SAS and Telco ACL Extended IP Filter entry form closes and the Manage 7250 SAS and Telco ACL Extended IP Filter form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

13 Close the Manage 7250 SAS and Telco ACL Extended IP Filter Policies form.

Procedure 48-6 To configure a 7250 SAS and Telco ACL IGMP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL IGMP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL IGMP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL IGMP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description
- Name

4 Click on the Filter Entries tab button.

5 Click on the Create button. The Entry, 7250 SAS and Telco ACL IGMP Filter (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Src Mask
- Destination IP
- Dest Mask
- Loggable
- IGMP Option

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The 7250 SAS and Telco ACL IGMP Filter (Create) form reappears.

11 To add more filter entries, repeat steps 5 to 10.

12 Click on the OK button to close the 7250 SAS and Telco ACL IGMP Filter (Create) form and save the policy.

13 Click on the Distribute button to manually distribute the policy locally to 7250 SAS or Telco devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

14 Click on the Selected radio button to choose from the listed devices.

15 Choose one or more rows from the Available Nodes list.

16 Click on the right arrow button. The selected devices move to the list on the right side of the form.

17 Click on the Distribute button. The policy is distributed to the device or devices.

18 Close the Distribute form. The 7250 SAS and Telco ACL IGMP Filter Policy form reappears.

19 Close the 7250 SAS and Telco ACL IGMP Filter Policy form. The Manage 7250 SAS and Telco ACL IGMP Filter Policies form reappears.

20 Close the Manage 7250 SAS and Telco ACL IGMP Filter Policies form.

Procedure 48-7 To configure a 7250 SAS and Telco ACL MAC filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL MAC Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL MAC Filter Policies form opens.

2 Perform one of the following:

  a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

  b Click on the Create button. The 7250 SAS and Telco ACL MAC Filter (Create) form opens.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Create button. The 7250 SAS and Telco ACL MAC Filter entry form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source MAC
- Destination MAC
- Pattern
- Src Mask
- Dst Mask
- Pattern Mask

The Pattern and Pattern Mask parameters are configurable when the check box is selected.

9 Click on the OK button.

10 To add more filter entries, repeat steps 5 to 11.

11 Click on the OK button. The 7250 SAS and Telco ACL MAC Filter (Create) form closes and the Manage 7250 SAS and Telco ACL MAC Filter Policies form reappears.

12 Click on the Search button to display the newly created policy or policies.

13 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

14 Close the Manage 7250 SAS and Telco ACL MAC Filter Policies form.

49 — Multicast policies

49.1 Multicast policies overview

You can use the 5620 SAM to create policies that regulate the flow of multicast traffic for more efficient multicast stream management, bandwidth management, traffic forwarding, and where multicast reports are sent.

Egress multicast groups

In VPLS standard multicasting, copies of the original packets are looped back to the SAP for transmission to each destination: an activity that consumes resources and makes the handling of congestion issues more difficult.

A more efficient method of forwarding multicast packets is to group destination SAPs in a set or "chain" that receives a single multicast packet from the egress forwarding plane with only a single pass. Adding SAPs to an EMG eliminates loopbacks by forwarding a multicast packet once to a group of shared definitions. As a result, an EMG makes multicasting more efficient and more scalable.

Creating an EMG in the 5620 SAM is similar to creating a policy, because it is first created globally and then distributed to NEs. The EMG is applied to an L2 access interface that has been created on an Ethernet port with null or dot1q encapsulation. SAP membership in an EMG has the following requirements:

- The SAP must belong to an SHG.
- The L2 access interface egress ACL filter must match that of the EMG.
- The access port and the EMG must have the same encapsulation type.

When a SAP becomes a member of an EMG, the common parameters that it shares with other EMG members cannot be changed. On the other hand, a modification to an EMG common requirement changes that parameter in all SAPs in the chain. The same common required traits apply to egress filters: individual SAP filters cannot be changed, and any change to the EMG egress filter parameters affects the egress filters in all member SAPs. In addition, if an egress filter is not defined in the EMG common parameter requirements, a new member SAP cannot have an egress filter.

The following restrictions also apply to an EMG:

- only IPv4 egress filters can be applied to an EMG
- up to 30 EMGs can be created on a router
- an EMG can be deleted only if it has no SAP members
- the number of members in an EMG (the chain limit) is restricted to 30, with an optimal length of 10 to 16

Multicast package policies

Multicast package policies for Telco devices group together BTV multicast streams which can be applied to Telco ring groups for distribution to end users.

Multicast package policies are also used to assign a common set of multicast groups to all 7450 ESSs and 7750 SRs in an MVR VPLS. Multicast package policies ensure that the multicast groups on the devices of one or more MVR VPLS instances are consistent. See chapter 30 for information about configuring multicast groups on individual devices using a multicast routing policy.

When a multicast package policy is distributed to a 7450 ESS or 7750 SR, a multicast routing policy is configured with the appropriate multicast prefix list, which is based on the multicast groups in the multicast package policy. Multicast package policies are only used to distribute the policies to one of the two NEs. Policy discovery and synchronization are not supported.

A multicast package policy has zero or more multicast groups associated with it. The multicast groups are distributed to the 7450 ESS or 7750 SR as part of the policy. Only root catalog multicast packages can be distributed to the 7450 ESSs or 7750 SRs.

Distributing multicast package policies

When you distribute a multicast package policy to a 7450 ESS or 7750 SR, the 5620 SAM maps one multicast package policy to one routing policy statement. Each multicast policy group entry is mapped to one routing policy prefix list member.

For example, the ID of a multicast package policy is 2. When the policy is distributed to a 7450 ESS or 7750 SR, the 5620 SAM automatically creates a routing policy statement for the device. The name created for the routing policy statement is SAM_MPP_2, where 2 is the multicast package policy ID.

When the policy is distributed to the 7450 ESS or 7750 SR, the ID of the routing policy statement entry is always 1. A name is generated by the 5620 SAM to identify the prefix list in the routing policy statement entry. The name is SAM_MPG_2_1, where 2 is the multicast package policy ID and 1 is the routing policy statement entry ID. The prefix list name is referenced in the routing policy statement entry as the multicast group prefix list name.

In the same example, the multicast address for the multicast group of a multicast package policy is 224.0.0.0. When the multicast package policy is distributed to a 7450 ESS or 7750 SR, the 5620 SAM automatically creates a routing policy prefix list member for the device. The prefix list member address is 224.0.0.0.

Since the multicast package policy is not resynchronized, you must avoid duplicate names for routing policies.

For the 7450 ESS and 7750 SR, if a multicast group does not have a policy group entry, the multicast group is not distributed to the device as a prefix member.

If a multicast package policy is used by any MVR VPLS, it cannot be removed from the 5620 SAM.

Multicast CAC policies

Multicast CAC policies control the bandwidth consumed by BTV distribution services. Bandwidth control helps manage network congestion and maintain QoS standards. The multicast CAC function is supported on any IGMP and PIM interface, and in the case of BTV distribution, on VPLS SAPs and SDPs where IGMP snooping is enabled.

A multicast CAC policy manages the bandwidth consumed by BTV services on both the access node link and specific links in the aggregation network. Routers in the path are configured to maintain certain limits on broadcast bandwidth and can limit the number of channels simultaneously sent on both the second mile link and the network link.

Multicast CAC policies are supported for VPLS on the 7710 SR, 7750 SR, and 7450 ESS.

Ingress Multicast Bandwidth policy

Ingress Multicast Bandwidth policies are used to manage the ingress multicast path bandwidth of the multicast forwarding paths into the switching fabric. When Multicast Path Management is disabled (the default), two paths are available:

- a high-priority path, on which packets from queues classified as “expedited” are forwarded
- a low-priority path on which packets from queues classified as “non-expedited” are forwarded

When Multicast Path Management is enabled, an Ingress Multicast Bandwidth policy can be used to manage the flow of multicast traffic through an MDA (IOM or IOM 2) or the forwarding plane of an 2 x XP MDA IOM 3 or IMM.

The maximum number of bandwidth policies per NE is 32, including the default policy.

MDAs can be configured to use previously defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress Multicast Info policy

Ingress Multicast Info policies are used to define how each multicast channel is handled by NEs. The policy is assigned to a VPLS/VPRN service site or default routing instance, but the policy is actually used by the Ingress Multicast Bandwidth Manager, the ECMP Path Manager, and the Egress Multicast CAC Manager to determine the path through the switch fabric and to make decisions on joins to multicast streams.

The maximum number of Info policies per NE is limited to 32, including the default policy.

MDAs can be configured to use previously-defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress multicast forwarding on L2-snooped and L3-routed IP multicast traffic can be explicitly configured by applying an Ingress Multicast Path Management Info policy to a VPLS site (all types of VPLS are supported), a VPRN site, or the default routing instance.

An Info policy consists of one or multiple named Bundles, which in turn, contain Channel ranges with possible overrides for individual channels.

Bundles

A Bundle groups a set of explicit multicast channels (or channel ranges) into a common bandwidth context for CAC functions (such as join decisions) using common preferences. The channels in the bundle are managed as a defined percentage of the available bandwidth.

Bundles also simplify provisioning, since the default characteristics of the bundle channels are specified on the bundle level. These characteristics can be overridden at the Channel range level, or explicitly per channel.

Each Info policy has a default bundle named “default”. It cannot be edited or removed. Any multicast channel that fails to match a channel range within an explicit operator-defined bundle is associated with this default bundle.

Note — The maximum number of Bundles per Info policies is limited to 32. This limit includes the default bundle, leaving 31 operator-defined bundles per Info policy.

Channels and channel ranges

Channel ranges are used to define a set of multicast channels contained in a bundle and to override the default channel settings in the containing bundle.

A channel range is defined by a start destination multicast IP address and an end destination multicast IP address (both IP v4 and IPv6 are supported, but the start and end addresses must be of the same type). A channel in this context is a channel range where the start address and end address are identical.

Note — After you create a channel range, it is not possible to modify the start address or end address.

A channel range can contain multiple channel overrides. A channel override is used to specify an explicit setting for a channel within the range. The channel override is identified by a destination multicast IP address which falls between the start and end IP addresses of the channel range.

Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

Dual stream selection

Dual stream selection support allows a single multicast stream to be duplicated into two different transmission paths. The two paths may have different transmission characteristics, such as latency and jitter. Rather than select one stream for retransmission to the client, the duplicate stream protection feature evaluates each stream packet-by-packet, selecting the packet that first arrives (and is valid) for retransmission.

Dual stream selection is supported on the 7710 SR and the 7750 SR.

Video quality monitoring

VQM to provides the functionality to analyze the quality of a video stream just prior to reaching the STB of client in a IPTV network. Statistics reports and alarms can be generated for VQM, providing operators with a view of multicast video quality at the last mile of distribution.

VQM is supported on the 7710 SR and the 7750 SR.

Ingress Multicast Reporting Destination policy

Ingress Multicast Reporting Destination policies are used to specify the destination server for the collection of multicast reports. The policies are applied to residential subscriber IGMP policies.

49.2 Multicast policies procedures

This section contains procedures relating to the configuration and maintenance of multicast policies.

Procedure 49-1 To create an egress multicast group policy

1 Choose Policies→Multicast→Egress Multicast Group. The Manage Egress Multicast Group Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

   b Click on the Create button. The Egress Multicast Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

   - Displayed Name
   - Description
   - Destination Chain Limit

4 Click on the SAP Common Requirements tab button.

5 Configure the parameters:

   - Encapsulation Type
   - Dot1 Q Ethertype
   - QinQ Ethertype
   - QinQ Fixed Tag Value

6 Click on the Select button in the Egress Filter panel to choose an egress policy. The Select Egress Filter search form opens.

7 Select an egress policy in the list and click on the OK button. The Select Egress Filter form closes and the egress policy information appears on the Egress Multicast Group (Create) form.

Note — The egress policy that you choose for this EMG must be the same as the egress policy specified for a member SAP.

8 Click on the Apply button to save the policy. The Egress Multicast Group (Create) form reappears with the General tab displayed.

9 Click on the More Actions button and choose Distribute to manually distribute the policy to local devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note 1 — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

Note 2 — To associate a SAP on the device with an EMG, the access port encapsulation type on the device must be the same as the encapsulation type that you specified in step 5.

10 Close the Egress Multicast Group form. The Manage Egress Multicast Group Policies form reappears.

11 Close the Manage Egress Multicast Group Policies form.

Procedure 49-2 To configure a multicast CAC policy

1 Choose Policies→Multicast→Multicast CAC. The Manage Multicast CAC Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Multicast CAC (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Action

4 Click on the Apply button. The Multicast CAC (Edit) form opens with the General tab displayed.

5 Click on the Bundles tab to associate a multicast bundle with the multicast CAC policy.

6 Click on the Create button. The Multicast CAC Bundle (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Max Bandwidth (kbps)
- Administrative State

8 Click on the Channels tab.

9 Click on the Create button. The Multicast CAC Channel (Create) form opens.

10 Configure the parameters:

- Start Address
- End Address
- Bandwidth (kbps)
- Class
- Type

11 Click on the OK button. The Multicast CAC Channel (Create) form closes and a dialog box appears.

12 Click on the OK button. The Multicast CAC Bundle (Create) form lists the newly configured channel.

13 To add additional channels to the bundle, repeat steps 9 to 12.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Multicast CAC Bundle (Create) form closes and the Multicast CAC (Edit) form reappears with the Bundles tab displayed.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Multicast CAC (Edit) form closes and the Manage Multicast CAC Policies form reappears.

18 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

19 Select a policy and click on the Distribute button to manually distribute the policy to local devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

20 Close the Manage Multicast CAC Policies form.

Procedure 49-3 To configure an Ingress Multicast Bandwidth policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Select the Multicast Bandwidth Policy (multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Bandwidth Policy from the contextual menu. The Multicast Bandwidth Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Falling Percent Reset (%)
- Admin BW Use Threshold (kbps)
- Percentage of Total pool (%)
- Reserved CBS (%)
- Displayed Name

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the T1 Paths tab button. A table displays the policy definitions for the primary, secondary, and ancillary paths. Each path definition contains configurable parameters.

6 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

7 Configure the parameters:

- Path Limit (mbps)
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

8 Click on the Apply button. A dialog box appears.

9 Click on the OK button.

10 Repeat steps 6 to 9 for the remaining paths, if required.

11 Click on the T2 Paths tab button. A table displays the policy definitions for the primary and secondary paths. Each path definition contains configurable parameters.

12 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

13 Configure the parameters:

- Number of Secondary T2 Paths
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

14 Click on the Apply button. A dialog box appears.

15 Click on the OK button.

16 Repeat steps 12 to 15 for the remaining path, if required.

17 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

18 Close the Multicast Bandwidth Policy form. The Manage Ingress Path Management Policies form reappears.

19 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 49-4 To configure an Ingress Multicast Information policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Choose Multicast Info Policy (Multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Info Policy from the contextual menu. The Multicast Info Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Bundles tab button. All defined bundles are displayed, including the default.

6 Click the Create button. The Info Policy Bundle, Multicast Info Policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Congestion Priority Threshold
- ECMP Optimization Threshold
- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

8 Click on the Video Defaults tab button.

9 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- (RT) Server
- Local Server

10 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 46 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

11 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

12 Click on the Tunnel Interfaces tab button.

13 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Bundle form opens.

14 Select a Multicast Path Management Bundle and click on the OK button.

15 The Select - Multicast Path Management Bundle form closes and the information is displayed.

16 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Bundle form opens.

17 Select an LDP Tunnel Interface and click on the OK button.

18 The Select LDP Tunnel Interface - Multicast Path Management Bundle form closes and the information is displayed.

19 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

20 Click on the Channels tab button.

21 Click the Create button. The Info Policy Channel Range, Info Policy Bundle (Create) form opens with the General tab displayed.

22 Configure the channel range parameters:

- Start Address
- End Address

Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

23 Configure any required overrides of the following parameters in the Channel Defaults block:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

24 Click on the Video tab button.

25 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- (RT) Server
- Local Server

26 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 46 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

27 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

28 Click on the Tunnel Interfaces tab button.

29 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

30 Select a Multicast Path Management Channel Range and click on the OK button.

31 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

32 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

33 Select an LDP Tunnel Interface and click on the OK button.

34 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

35 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

36 Click on the Channel Override tab button if you need to specify overrides for explicit channels within the Channel Range.

37 Click on the Create button. The Info Policy Channel Override (Create) form opens, with the General tab displayed.

38 Enter the Source Address of the channel for which you want to specify overrides.

39 Configure any required overrides of the following parameters for the channel in the Overrides block:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

40 Click on the OK button. A dialog box appears. Click OK. The channel to which you applied overrides is displayed.

41 Click on the Video tab button.

42 Configure the parameters:

- Video Group ID
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size
- (RT) Server
- Local Server

43 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 46 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

44 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax parameter.

vi Enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

45 Click on the Tunnel Interfaces tab button.

46 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

47 Select a Multicast Path Management Channel Range and click on the OK button.

48 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

49 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

50 Select an LDP Tunnel Interface and click on the OK button.

51 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

52 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

53 Click on the Video Interfaces tab button if you need to configure a video interface.

Note — If you are configuring a video interface you must perform the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the video interface are retained. See chapter 46 for information on policy distribution modes. See chapter 36 for more information about IPTV video features and configuration.

54 Click on the Create button. The Multicast Video Interface (Create) form opens with the General tab displayed.

55 Configure the Address parameter.

56 Click on the Channel Config tab button.

57 Select a channel in the list and click on the Properties button. The Multicast Video Interface Channel Config (Create) form opens.

58 Configure the parameters:

- RT Rate
- Local Retransmission Server
- RT Payload Type
- FCC Server Mode
- FCC Burst
- FCC MC Handover Rate
- Max IGMP Latency
- Max Number of Sessions

59 Click on the OK button. The Multicast Video Interface Channel Config (Create) form closes and a dialog box appears.

60 Click on the OK button. The configured channels are displayed in the list.

61 Repeat steps 56 to 60 to configure additional channels, if required.

62 Click on the OK button. The Multicast Video Interface (Create) form closes and a dialog box appears.

63 Click on the OK button.

64 Click on the Apply button.

65 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

66 You can view information on VPLS sites (regular sites and I-Sites), VPRN sites, and Default Routing Instances affected by the Multicast Info Policy by clicking the appropriate tab. Run a search and view the properties for the desired item.

67 Close the Multicast Info Policy form. The Manage Ingress Path Management Policies form reappears.

68 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 49-5 To create or edit an ingress multicast reporting destination policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Select Multicast Reporting Destination (Multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Multicast Reporting Destination from the list. The Multicast Reporting Destination, Global Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Destination Address
- Destination UDP Port
- Max Delay (Deciseconds)
- Administrative State

5 Click on the Apply button to save the policy. The Multicast Reporting Destination, Global Policy (edit) form appears with the General tab displayed.

6 Click on the More Actions button and choose Distribute to manually distribute the policy to local devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

7 Close the Multicast Reporting Destination, Global Policy (edit) form.

8 Close the Ingress Path Management Policies form.

Procedure 49-6 To configure a Multicast SSM Translate policy

Source-Specific Multicast allows the receiver of multicast packets to specify desired source addresses to the router, so that only packets originating from the specified sources are delivered. IGMP is used by the client to inform the router of the specified addresses.

The SSM Translate Policy allows you to create global sets of SSM Translate Items that can be mass-delivered to many routers at once. Every policy has one or more SSM Translate Items. When the policy is distributed, all of these items are deployed to the target base routers.

Note — IGMP must be enabled on the routers to which you intend to distribute the SSM Translate policy.

1 Choose Policies→Multicast→SSM Translate. The SSM Translate Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The SSM Translate Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the SSM Translate Items tab. All defined SSM Translate Items are displayed.

5 Click the Create button. The SSM Translate Policy Item (Create) form opens.

6 Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source

Note — The SSM Translate Items added to a policy should not have overlapping IPv4 address ranges, otherwise a configuration error message will be issued.

7 Click OK. An information dialog box is displayed. Click OK.

8 Click the Apply button.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note 1 — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See Procedure 46-1 for more information.

Note 2 — When you distribute an SSM Translate policy to a router, it replaces any SSM Translate policy that may exist on that router. All existing SSM Translate Items on the router will be overwritten.

10 Close the SSM Translate Policy (Create) form. The SSM Translate Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 49-7 To view NE multicast reporting destination statistics

Perform this procedure to view multicast reporting destination statistics for a particular NE. This procedure allows you to display useful information including frames and records lost and sent. See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Ingress Path Management Policies form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button to select an NE. The Select a Network Element form opens.

4 Choose an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

5 Choose Multicast Reporting Destination (Multicast) from the object drop-down list.

6 Specify a filter to search for an existing policy.

7 Choose a policy from the list and click on the Properties button. The Multicast Reporting Destination, Local Policy (Edit) form opens.

8 Click on the Statistics tab button.

9 Click on the Collect button to collect on-demand statistics.

10 Choose a statistics record and click on the Properties button to view the record. The Statistics Record - Multicast Reporting Destination Stats form opens.

11 View the statistics information.

12 Close the statistics record form.

13 Close other open forms, as required.

Procedure 49-8 To view multicast CAC channel statistics

Perform this procedure to view multicast CAC channel statistics and identify the status of BTV channels on a managed NE. This procedure allows you to display useful information including which channels are blocked and their location, bandwidth availability, the number of times channel requests are dropped on an interface, and the cause of the action based on the multicast CAC policy. See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Tools→BTV Channel Monitor. The Select Site form opens.

2 Select a site in the list and click on the OK button. The BTV Channel Monitor form opens.

3 Perform one of the following:

a Choose Multicast CAC Channel Statistics (multicast) from the object drop-down list to list network protocol statistics.

b Choose Multicast CAC Channel Statistics on Services (multicast) from the object drop-down list to list service statistics.

4 Configure the filter criteria and click on the Search button. A list of multicast CAC channel statistics is displayed at the bottom of the form.

Note — To get the most recent channel information on a managed NE, perform a resynchronization by clicking on the Resync button before clicking on the Search button.

5 Close the BTV Channel Monitor form.

Procedure 49-9 To configure a multicast package policy

Use multicast package policies to:

- define a set of broadcast channels that are multicast across a ring group in a BTV VLAN
- assign a common set of multicast groups to all 7450 ESSs or 7750 SRs in an MVR VPLS to ensure accuracy and consistency

Consider the following when creating multicast package policies:

- one root multicast package policy should be created for a ring or multiple rings, which contains the multicast addresses of all BTV channels distributed in the ring
- specify this root multicast package policy for the BTV (MVR) VLAN
- create other multicast package policies from the root package by clicking on the More Actions button and choosing Copy on the configuration form
- use the child policies to differentiate the types of broadcast TV services offered, for example, basic service and premium service
- when you create 7250 SAS and Telco IGMP ACL filter policies, use these child policies to limit access for end users to specific types of services, for example, access to basic service, premium service, or both services

1 Choose Policies→Multicast→Multicast Package from the 5620 SAM main menu. The Multicast Package Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Multicast Package Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Name
- Description
- Is Root Catalogue
- IGMP Option
- Loggable

4 Click on the Multicast Groups tab button.

5 Click on the Create button. The Multicast Group (Create) form opens.

Note — Each multicast group that is specified must be preconfigured in the PIM configuration. See the PIM configuration procedures in chapter 31.

6 Configure the parameters:

- Multicast Address
- Name
- Description
- Channel
- Cost

7 Click on the Apply button to save the policy. The Multicast Package Policy (Create) form is refreshed with additional buttons.

8 Click on the Definitions tab, if applicable.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices in the ring. You can use the Distribute button when the Is Root Catalogue parameter is set to root. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

When any new devices are added to the ring, the policy is automatically distributed to any new MVR VLAN service or to any new MVR VLAN service sites in the ring.

10 Click on the Selected radio button to choose from the listed devices.

11 Choose one or more rows from the Available Nodes list.

12 Click on the right arrow button. The selected devices move to the list on the right side of the form.

13 Click on the Distribute button. The policy is distributed to the device or devices.

14 Close the Distribute form. The Multicast Package Policy form reappears.

15 Close the Multicast Package Policy form.

Create other multicast package policies from the root policy by clicking on the More Actions button and choosing Copy, as required. These child policies of the root policy can be used to help differentiate the types of BTV services being created, for example, basic services and premium services.

50 — Time of day policies

50.1 Time of day policies overview

The 5620 SAM supports the creation of time of day policies that allow you to configure time-based QoS policies, ACL filters, and schedulers that are applied to aggregation schedulers and L2 and L3 access interfaces. For example, a time of day policy allows you to manage peer-to-peer traffic by limiting access during peak hours, such as evenings and weekends.

A time range policy consists of one or more schedules, which include a start and end day and time and a priority.

A time of day suite policy is a collection of ingress and egress policies, filter policies, and schedulers, to which time range policies have been assigned. You can apply time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

You can create a time of day suite policy by assigning time range policies to the following objects to apply time and day restrictions to their deployment and access:

- ACL MAC filters and filter entries
- ACL IP filters and filter entries
- ACL IPv6 filters and filter entries
- access ingress and egress QoS policies
- scheduler policies

The default time range policy is the NO-TIME-RANGE policy, which means that no time and day restrictions apply. There can be only one NO-TIME-RANGE entry in each type of time of day suite policy entry.

Time range policies are first created globally and then distributed to NEs. You can distribute time range policies to the 7210 SAS-D 6F 4T, 7210 SAS-D 6F 4T ETR, 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7710 SR, and 7750 SR.

Time range assignment analysis tool

The time range assignment analysis tool allows you to view the time range policies that have been assigned over a specific time period to the following objects:

- L2 access interfaces
- L3 access interfaces
- aggregation schedulers
- time of day suite policies

You can use the time range assignment analysis tool to verify the configuration of multiple schedules and the adequacy of a time of day suite policy on a specific NE. For example, you can use this tool to verify that multiple time ranges that are assigned to IP filters in a time of day suite policy cover an entire month.

50.2 Time of day policies procedures

The following procedures describe how to configure and manage time of day policies.

Procedure 50-1 To configure a time range policy

1 Choose Policies→Time of Day→Time Range from the 5620 SAM main menu. The Manage Time Range form opens.

2 Perform one of the following:

 a Specify a filter to search for an existing time range policy. Select a policy in the filtered list and click on the Properties button.

 b Click on the Create button. The Time Range (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the Time Range Entries tab button.

5 Click on the Create button. The Time Range Entries (Create) form opens.

6 Configure the parameters:

- Start Time
- End Time
- Ongoing
- Frequency
- Start Run Day
- End Run Day

The Frequency parameter is configurable when the Ongoing parameter is enabled.

The Start Run Day and End Run Day parameters are configurable when the Frequency parameter is set to Weekly.

7 Click on the OK button. The Time Range Entries (Create) closes. The Manage Time Range form opens.

8 Click on the Search button to display the newly created policy or policies.

9 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

10 Close the Manage Time Range form.

Procedure 50-2 To configure a time of day suite

Consider the following when you create a time of day suite policy:

- when there are overlapping time range policy entries within a time of day suite policy, the time range policy entry with the highest priority is applied first
- only one time of day suite policy entry without a time range (default NO-TIME-RANGE) is allowed for each type of policy
- you cannot modify a time of day suite policy entry after you create the entry
- you cannot assign the same priority of a global policy within the same policy type
- you cannot assign the same priority of a local policy within the same policy type
- you cannot assign the same time range of a global policy within the same policy type
- you cannot assign the same time range a local policy within the same policy type
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same time range as the global policy
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same priority as the global policy
- all time of day suite policy entries of a local policy are replaced by the time of day suite policy entries of a global policy if none of the entries from the local policy have the same priority or time ranges as the global policy

1 Choose Policies→Time of Day→Time Of Day Suite from the 5620 SAM main menu. The Manage Time-of-day suite form opens.

2 Perform one of the following:

a Specify a filter to search for an existing suite. Select a suite in the filtered list and click on the Properties button.

b Click on the Create button. The Time of Day Suite (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the TOD Suite Entries tab button.

5 Click on the Ingress tab button.

6 Assign a time range to ingress filter policies, if required. Perform the following steps:

i Click on the Create button. The Ingress *type_of_filter* (Create) form opens.

ii Configure the Priority parameter.

iii Click on the Select button beside the Name parameter. The Select Time Range - Ingress *filter* list form opens.

iv Select a time range in the list and click on the OK button. The Select Time Range - Ingress *filter* list form closes.

v Click on the Select button beside the Filter ID parameter. The ingress filter list form opens.

vi Select a filter in the list and click on the OK button. The ingress filter list form closes.

vii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

7 Assign a time range to ingress QoS policies, if required. Perform the following:

i Click on the QoS tab button.

ii Click on the Create button. The Ingress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Ingress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Ingress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Ingress QoS list form closes.

viii Click on the Select button in the 7210 Policy panel. The Select 7210 Policy - Ingress QoS list form opens.

ix Select an entry in the list and click on the OK button. The Select 7210 Policy - Ingress QoS list form closes.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Time of Day Suite (Create) form reappears.

8 Assign a time range to ingress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab button.

ii Click on the Create button. The Ingress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Ingress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Ingress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Ingress Scheduler list form closes.

viii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

9 Click on the Egress tab button.

10 Assign a time range to egress filter policies, if required. Perform the following steps:

i Click on the Create button. The Egress *type_of_filter* (Create) form opens.

ii Configure the Priority parameter.

iii Click on the Select button beside the Name parameter. The Select Time Range - Egress *filter* list form opens.

iv Select a time range in the list and click on the OK button. The Select Time Range - Egress *type_of_filter* list form closes.

v Click on the Select button beside the Filter ID parameter. The egress filter list form opens.

vi Select a filter in the list and click on the OK button. The egress filter list form closes.

11 Assign a time range to egress QoS policies, if required. Perform the following:

i Click on the QoS tab button.

ii Click on the Create button. The Egress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Egress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Egress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Egress QoS list form closes.

12 Assign a time range to egress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab button.

ii Click on the Create button. The Egress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Egress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Egress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Egress Scheduler list form closes.

13 Click on the OK button. The Time of Day Suite (Create) form closes and the Manage Time-of-day suite form reappears.

14 Close the Manage Time-of-day suite form.

Procedure 50-3 To perform a time range entry assignment analysis

1 Choose Tools→Time Range Entry Assignment from the 5620 SAM main menu. The List Time Range Entry Assignment form opens.

2 Click on the Select button to choose a site for the analysis. The Select Site to Analyze form opens.

3 Select a site in the list and click on the OK button.

4 Configure the Time Range Entry Container Type parameter.

5 Click on the Select button beside the Time Range Entry Container Type to choose a specific object of the container type you chose in step 4. The appropriate list form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The list form closes and the List Time Range Entry Assignment form refreshes.

9 Configure the Search by TIme Of Day Entry Type and Time Of Day Entry Policy Type parameters.

10 Configure the Start Date and End Date parameters.

11 Click on the Search button. A list of time range entries that meet the defined criteria is displayed.

12 Double-click on an entry to view information about the time range policy and time of day suite policy. The Time Range Entry Assignment: *Start Date End Date* form opens.

13 Click on the Cancel button to close the Time Range Entry Assignment: *Start Date End Date* form.

14 Close the List Time Range Entry Assignment form.

51 — VRRP policies

51.1 VRRP policies overview

VRRP priority control-policies manage VR backup router priorities. The policies override the base priority value, depending on NE events or conditions. You can configure a VRRP policy only for the non-owner VRRP instance; the same policy can be applied to IPv4 and IPv6 VRRP instances.

The main function of a VRRP priority-control policy is to define the conditions or events that affect the VR ability to communicate with outside hosts or portions of the network. When at least one of these events is true, the base priority for the VR instance is affected in one of two ways:

- an explicit value is overridden
- a value is subtracted from the sum of delta priorities

The result is the actual in-use priority for the VR instance. Any priority event may be configured as an explicit event or a delta event.

Table 51-1 describes the policy events that you can configure using the 5620 SAM.

Table 51-1 VRRP policy events

Policy Event	Description
Host unreachable	Configures a host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IP host address. A host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IP address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
IPv6 Host unreachable	Configures an IPv6 host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IPv6 host address. An IPv6 host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IPv6 address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
LAG port down	Configures a LAG priority-control event that monitors the operational state of the links and each port in the LAG. When one or more of the ports enters the operational down state, the event is considered to be set. When all ports enter an operational up state, the event is considered to be clear.
Route unknown	Configures a route unknown priority-control event that monitors the existence of a specific active IP route prefix in the routing table. Route unknown defines a link between the VRRP priority-control policy and the RTM. The RTM registers the specified route prefix as monitored by the policy. If any change (add, delete, new next hop) occurs relative to the prefix, the policy is notified and takes action according to the priority event definition.
Port Down Events	Configures an override or adjustment to the base priority value of a VRRP VR instance depending on the operational state of the event. Port Down events can only be configured on the local definitions of VRRP policies.

As priority events clear in the policy, the in-use priority can eventually be restored to the base priority value.

51.2 VRRP policies procedures

The following procedures describe how to configure and manage VRRP policies.

Procedure 51-1 To configure a VRRP priority-control policy

1 Choose Policies→VRRP from the 5620 SAM main menu. The Manage VRRP Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The VRRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Delta in Use Limit

4 Click on the Apply button.

5 Perform one of the following steps:

a For IPv4 hosts, click on the Host Unreachable tab button.

i Click on the Create button. The Host Unreachable Event (Create) form opens.

ii Configure the parameters:

- IP Address
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority Type
- Priority
- Limit of Echo Request Failures
- Interval for Echo Request (seconds)
- Timeout for Echo Request (seconds)

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Host Unreachable Event form reappears with the newly created filter entries displayed.

v Go to step 6.

b For IPv6 hosts, click on the IPv6 Host Unreachable tab button.

i Click on the Create button. The IPv6 Host Unreachable Event (Create) form opens.

ii Configure the parameters:

- IP Address
- Interface Name
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority Type
- Priority
- Limit of Echo Request Failures
- Interval for Echo Request (seconds)
- Timeout for Echo Request (seconds)

The Interface Name parameter is only configurable when the host IP Address parameter is a Link Local Address.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The IPv6 Host Unreachable Event form reappears with the newly-created filter entries displayed.

v Go to step 6.

6 Click on the Lag Port Down tab button.

7 Click on the Create button. The Lag Port Down Event (Create) form opens with the General tab displayed.

8 Configure the parameters:

- LAG ID
- Hold Clear (seconds)
- Hold Set (seconds)

9 Click on the Number Down tab button.

10 Click on the Create button. The Number Down (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Number of Ports Down
- Priority
- Priority Type

12 Close the Number Down (Create) form. A dialog box appears.

13 Click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Lag Port Down Event form reappears with the newly created filter entries displayed.

16 Click on the Route Unknown tab button.

17 Click on the Create button. The Route Unknown (Create) form opens with the General tab displayed.

18 Configure the parameters:

- IP Address
- Mask
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority
- Priority Type
- Protocol
- Less Specific

19 Click on the Next Hop tab button.

20 Click on the Create button.

If the IP Address you specify on the General tab is an IPv4 address, the NextHop (Create) form opens; if it is an IPv6 address, the NextHopV6 (Create) form opens.

21 Configure the Hop Address parameter.

22 Configure the Interface Name parameter if the IPv6 Next Hop Address is a Link Local Address.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button.

25 Click on the OK button.The Manage VRRP Policies form reappears.

26 Click on the Search button to display the newly created policy or policies.

27 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

28 Close the Manage VRRP Policies form.

52 — Auto tunnels policies

52.1 Auto tunnels policies overview

The 5620 SAM supports the creation of service tunnels for groups of NEs based on mesh, hub-and-spoke, or ring network topology. The 5620 SAM uses tunnel management policies to define the conditions for service tunnel creation. A tunnel management policy has four components:

- the group of NEs to which the policy applies and their collective role
- the tunnel specifications, for example, the tunnel type and underlying transport
- the topology specification, for example, mesh
- a tunnel template must be applied

You can specify a system-generated naming format, or you can also specify a naming prefix. The resulting name is a combination of the user-specified prefix and the ID of the tunnel.

Tunnel templates

You must create a tunnel policy using a tunnel template. You can view, but not save or reapply, a tunnel policy created using 5620 SAM releases earlier than 7.0. For example, if a new tunnel is required as a result of group member changes, the tunnel cannot be created if the policy was created using a 5620 SAM release earlier than 7.0. If such a tunnel must be deleted as a result of group member changes, the tunnel can be deleted regardless of the state of the policy.

Depending on the tunnel type selected for an auto tunnel, an SDP or LSP tunnel template can be selected. For an RSVP LSP tunnel type, one LSP template must be selected. For an RSVP SDP tunnel type, 16 LSP templates can be selected. When an LSP parent template with more than one LSP path child templates is specified, more than one LSP path is created.

A template should be configured to be deployed to a majority of the NE types. The user must validate the template and enter appropriate changes to the script before the template can be deployed in an auto tunnel policy. The parameters that can be modified, depend on the template type.

The following parameters can be modified for an SDP template:

- name
- source NE ID
- destination NE ID
- displayed name
- LDP enabled
- underlying transport
- path ID

The following parameters can be modified for an LSP template:

- name
- source NE ID
- path ID
- displayed name

- destination IP address
- destination NE ID

Note — If the policy ID value is specified by a format policy in the template, the path ID value must be set to 0.

When you execute an LSP path template in an auto tunnel policy, the following parameters are substituted with the values from the original tunnel policy:

- name
- resource ID

You can create templates from examples. Use an example as a starting point to create service or tunnel templates with or without format and range policies. When a template with format and range policies is associated with an auto tunnel rule, the format and range policies defined in the template override the name defined in the auto tunnel rule.

Class of Service

When you implement CoS, consider the following:

- To create a CoS-based SDP using RSVP, a user must apply a combination of SDP and LSP templates. An SDP tunnel template can use up to 16 LSPs. For CoS routing, 10 LSP s are required for the following: 1 for default, 1 for multicast, and 8 LSPs for different CoS routes.
- For CoS-based forwarding, at least one LSP template must be associated with the SDP. The LSP template must be specified as the default LSP template for CoS forwarding.
- When LSP templates are not specified, during non-CoS-based forwarding, the SDPs are created without LSPs attached.

Tunnel groups

A tunnel group is defined as collection of network resources, such as NEs, that perform the same role in the network; for example, the way that the designation of a port as an access or network port defines the role of the port in the network.

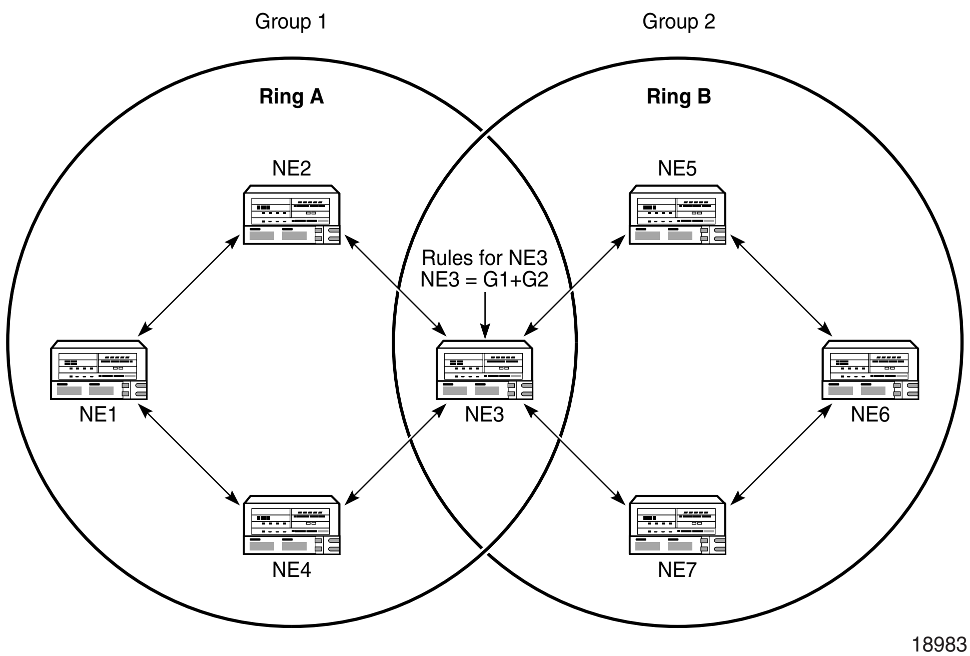
By grouping resources by role, a common policy-based management framework can be used to ensure the appropriate configuration of resources, for example, create service tunnels for different topologies.

The following conditions apply to tunnel groups.

- An NE can belong to multiple groups.
- A group is ordered or unordered depending on the requirements. The members in a group must be ordered when you create some topologies; for example, a ring topology. Topologies such as mesh or hub-and-spoke, in which NEs are not linearly arranged, do not need an ordered group.

- A non-5620 SAM-managed NE can belong to the tunnel group to which it was added, however, it is not active as a destination NE during rule execution.
- When two or more tunnel groups share an NE, the shared NE performs the roles defined for each group. In Figure 52-1, Group 1 contains routers NE1, NE2, NE3, and NE4, and Group 2 contains routers NE3, NE5, NE6, and NE7. NE3 is the intersection set of Groups 1 and 2, therefore NE3 assumes the roles defined for Groups 1 and 2.

Figure 52-1 NE shared by two tunnel groups



Tunnel policy creation requires the configuration of the following:

- one or more group conditions to specify the NEs that are included in the topology
- a least one tunnel template configuration
- one or more tunnel definitions that specify the service-tunnel characteristics, such as the type of tunnel and the underlying transport

Tunnel policy rules

The following conditions apply to tunnel policies.

- A 5620 SAM operator requires topology-management privileges to create or modify a tunnel policy.
- A tunnel can originate and terminate on 5620 SAM-managed NEs. Tunnels cannot originate on non-SAM-managed NEs, however, tunnels can terminate on non-SAM-managed NEs.
- When an NE, that is in a rule-based group, is unmanaged or delete, it is identified as unmanaged in the rule-based group. Tunnels to the NE are not removed, however tunnels from the NE are removed from 5620 SAM.

- When an auto-tunnel rule is created for a group that contains non-SAM-managed NEs, tunnels cannot be created to and from the NE using that rule.
- When you add NEs to a tunnel group that is in use, new tunnels are created according to the policy definition.
- A group condition must contain at least one group of NEs.
- Tunnel elements are not updated dynamically.
- An unmanaged NE is removed from the tunnel groups to which the NE belongs. The associated service tunnels are also removed if they originate from a managed NE. A service tunnel that originates on an unmanaged NE is retained, but is not included in the tunnel group after reconfiguration.
- When a service tunnel created by a tunnel policy is removed, the policy does not attempt to recreate the tunnel.
- You can modify the tunnel definition in a tunnel policy when the tunnel policy has not yet created a service tunnel.

Not all NEs that are assigned to a topology rule share the same functionality. The topology rule runs capability checks on the source NEs to determine whether specific tunnels or tunnel configurations can be applied. Table 52-1 lists the auto tunnel rules that are supported by each NE.

Table 52-1 Auto tunnel rules and NE support

Auto tunnel rule	7710 SR 7450 ESS 7750 SR	7705 SAR			7250 SAS-ES
		1.0	1.1	2.0	
SDP LDP	X	X	X	X	—
SDP GRE	X	—	X	X	—
SDP LSP	X	X	X	X	X
Dynamic LSP	X	—	—	X	X
CoS-based SDP	X	—	—	—	—
LDP-over-RSVP	X	—	—	—	—

52.2 Workflow to configure auto tunnel creation

Perform the following steps to configure an auto tunnel.

1. Configure a tunnel template from one of the following:
   - template creation form
   - network or service object properties form
   - pre-configured tunnel template

   See the *5620 SAM Scripts and Templates Developer Guide* for more information.

2. Configure rule-based groups. See Procedure 52-1 for more information.

3 As required, convert an auto tunnel rule created using a release of the 5620 SAM earlier than release 7.0 to a template-based auto tunnel rule. See Procedure 52-2 for more information.

4 As required, configure mesh or ring topology rules. See Procedure 52-3 for more information.

5 As required, configure hub and spoke topology rules. See Procedure 52-4 for more information.

6 As required, import tunnels not managed by topology rules. See Procedure 52-6 for more information.

7 Execute a topology rule. See Procedure 52-8 for more information.

8 As required, display missing tunnel elements. See Procedure 52-9 for more information.

9 Create a service and specify Automatic Mesh SDP Binding Creation. See the appropriate service chapter for more information.

52.3 Auto tunnels policies procedures

The following procedures describe how to configure and manage auto tunnel elements.

Procedure 52-1 To create a rule-based group

1 Choose Policies→Auto Tunnels→Rule-Based Groups from the 5620 SAM main menu. The Manage Rule-Based Groups form opens.

2 Click on the Create button and choose Create Rule-Based NE Group from the menu. The Rule-Based NE Group (Create) form opens.

3 Configure the parameters.

- Group Name
- Description
- Order

4 Click on the Apply button to save the changes. The Group Members tab becomes configurable.

5 Click on the Group Members tab button.

6 Depending on the value specified for the Order parameter, perform one of the following:

a Add members to an unordered group.

i Click on the Create button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add another member to the unordered group, if required or go to step 7.

b Add members to an ordered group.

i Click on the Create button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add a member to the end of the ordered group list, if required.

v To insert an NE between two NEs in the ordered group list, click on the Insert button and perform steps 6ii to iii.

7 Click the OK button. A dialog box appears.

8 Click the Yes button. The Rule-based NE Group (Edit) form closes and the Manage Rule-Based Groups form reappears.

9 Close the Manage Rule-Based Groups form.

Procedure 52-2 To convert old auto tunnel rules to template-based auto tunnel rules

Perform this procedure to convert tunnel policies created using a 5620 SAM Release earlier than 7.0 to template-based auto tunnel rules.

The number and type of templates that are displayed depend on the policy type. For example, a mesh SDP policy with GRE as the underlying transport requires 1 SDP template. A hub-and-spoke SDP policy with LSP as the underlying transport requires two SDP and two LSP templates.

When you apply a new template to an old auto tunnel rule, you must ensure that the parameter values defined in the template are consistent with the values that you defined in the original auto tunnel rule. For example, if you convert an auto tunnel rule that requires you to apply an LSP template, you must choose a template in which the LSP Bandwidth and Fast Re-Route parameter values in the template match the values defined in the old auto tunnel rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Search button. A list of old and new auto tunnel rules is displayed.

3 Select an old auto tunnel rule in the list.

4 Click on the Properties button. An *Auto Rule_type* (Edit) form opens.

5 Click on the More Actions button and choose Convert. The Convert Old Rule form opens.

Note — The Convert option is displayed only if the selected policy has been created using a 5620 SAM Release earlier than 7.0.

6 Perform one or both of the following, depending on the type of tunnel and the underlying transport value.

When the tunnel type value is SDP and the underlying transport value is RSVP-LSP, you must choose a SDP and an LSP template. When the tunnel type value is LSP, you must choose an LSP template only.

a Click on the Select button beside the Name parameter in the SDP Template panel. The Select Template form opens.

b Click on the Select button beside the Name parameter in the LSP Template panel. The Select Template form opens.

7 Select a template in the list and click on the Execute button. The Convert Old Rule form is refreshed with the template information and the Execute button is replaced with a Done button.

Note — After an auto tunnel rule is converted, the Convert option is not displayed when the *Auto Rule_type* (Edit) form is opened.

8 Click on the Tunnel Definition tab in the *Auto Rule_type* (Edit) form. The Template panel is refreshed with the template information.

9 Close the Convert Old Rule form and close the *Auto Rule_type* (Edit) form.

Procedure 52-3 To create a mesh or ring topology rule

Perform this procedure to create a mesh topology rule for service-tunnel creation. A template must be applied to an auto-tunnel policy. You must configure an LSP or SDP tunnel template before you can deploy a template to an LSP or SDP tunnel. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel templates.

Note — You must convert auto tunnel rules created using a 5620 SAM release earlier than 7.0 if the auto tunnels are not associated with a tunnel template. See Procedure 52-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose one of the following:

- **a** Create Mesh Topology Rule. The Mesh Topology Rule (Create) form opens with the General tab displayed.
- **b** Create Ring Topology Rule. The Ring Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the LERs Definition tab button.

5 Click on the Add button. The Select Rule-Based Group form opens.

6 Click on the Search button.

7 Select a rule-based group in the list and click on the OK button. The Select Rule-Based Group form closes and the group is displayed on the Topology Rule (Create) form.

8 Click on the Tunnel Definition tab button.

9 Perform one of the following to configure the Tunnel Type parameter:

- **a** Choose SDP.
- **b** Choose RSVP-LSP; go to step 19.

10 Click on the SDP tab button.

11 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

12 Select a template in the list. See Procedure 6-3 for information about creating a tunnel template.

13 Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Topology Rule (Create) form.

14 Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State
- Import Administrative Groups

The Class Forwarding Capability and Administrative State parameters are configurable when the Underlying Transport parameter is set to RSVP-LSP.

The Administrative State parameter is not configurable when the Class Forwarding Capability parameter is disabled.

15 If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab button; otherwise, go to step 22.

16 Click on the Add button. The Select LSP Template form opens.

17 Select a template in the list and click on the OK button. The Select LSP Template form closes and the Topology Rule (Create) form displays the LSP template information.

18 Go to step 22.

19 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

20 Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Topology Rule (Create) form.

21 Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 52-4 To create a hub-and-spoke topology rule

Note — You must convert auto tunnel rules created using a 5620 SAM release earlier than 7.0 if the auto tunnels are not associated with a tunnel template. See Procedure 52-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose Create Hub and Spoke Topology Rule from the contextual menu. The Hub and Spoke Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the Hub LERs Definition tab button.

5 Click on the Add button. The Select form opens.

6 Click on the Search button. A list of rule-based groups is displayed.

7 Select a group in the list and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

8 Click on the Spoke LERs Definition tab button.

9 Click on the Add button. The Select form opens.

10 Click on the Search button. A list of rule-based groups is displayed.

11 Select a group and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

12 Click on the Hub Tunnel Definition tab button.

13 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 16.

14 Click on the SDP tab button.

15 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

i Select a template in the list.

ii Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iii Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State
- Import Administrative Groups

The Class Forwarding Capability and Administrative State parameters are displayed when the Underlying Transport parameter is set to RSVP-LSP.

The Administrative State parameter is configurable when the Class Forwarding Capability parameter is enabled.

iv If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab button; otherwise go to step 18.

v Click on the Add button. The Select LSP Templates form opens.

vi Select a template in the list and click on the OK button. The Select LSP Templates form closes and the Associated LSP Templates panel displays the LSP template information.

vii Select the LSP template in the Associated LSP Templates panel. If the Class Forwarding Capability parameter in step 15 is enabled, the buttons in the Class Forwarding panel become enabled; otherwise, go to step 18.

viii Click on the Set as Default LSP button to specify the LSP as the default, if required.

ix Click on the Set as Multicast LSP button to specify that the LSP is a multicast LSP, if required.

x Click on the Choose a Forwarding Class button and choose a forwarding class from the contextual menu, if required.

16 Click on the LSP tab button.

17 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

i Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

ii Configure the Enable LDP-over-RSVP parameter.

18 Click on the Spoke Tunnel Definition tab button.

19 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 21.

20 Perform the following steps.

i Click on the SDP tab button.

ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

iii Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iv Configure the Underlying Transport parameter.

21 Perform the following steps.

  i Click on the LSP tab button.

  ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

  iii Select a template in the list and click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

  iv Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Hub and Spoke Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 52-5 To modify a topology rule

Use this procedure to change the parameter settings for a topology rule.

Note — You can modify group conditions and tunnel definitions only when a topology rule is not active.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button.

3 Select a rule and click on Properties. The system displays the rule properties form.

4 Make the required changes to the rule.

5 Click on OK button. A dialog box appears.

6 Click the Yes button. The rule properties form closes and the Manage Auto Tunnel Rules form reappears.

7 Close the Manage Auto Tunnel Rules form.

Procedure 52-6 To import tunnels not managed by topology rules

Use this procedure to import a tunnel that is not managed by a topology rule. After you import the tunnel, the tunnel is manage by the rule. However, the rule does not enforce the source and destination IDs to match the rule group. If the imported tunnel is not part of the group, the execute button or change notifications by the group members do not apply, even though the imported tunnel is part of the rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of auto tunnel rules is displayed.

3 Select a rule in the list and click on the Properties button. The system displays the *Topology_Rules* (Edit) form.

4 Click on the Created/Imported Tunnel Elements tab button.

5 Click on the More Actions button and choose Import Tunnels. An Import Tunnels form opens.

6 Perform one of the following:

- **a** Click on the Add SDPs button. The Select SDPs form opens. Go to step 8.
- **b** Click on the Add LSPs button. The Select LSPs form opens.

7 Click on the Search button. A list of LSPs is displayed.

- **i** Choose one or more LSPs in the list.
- **ii** Click on the OK button. The Select LSPs form closes and the Import Tunnels form is refreshed with the chosen LSPs. Go to step 9.

8 Click on the Search button. A list of SDPs is displayed.

- **i** Choose one or more SDPs in the list.
- **ii** Click on the OK button. The Select SDPs form closes and the Import Tunnels form is refreshed with the chosen SDPs.

9 Click on the Import button. The Import Tunnels form closes.

10 Click on the Created/Managed Tunnel Elements tab button to view the imported networks.

11 Close the *Topology_Rules* (Edit) form.

12 Close the Manage Auto Tunnel Rules form.

Procedure 52-7 To display and delete tunnel elements

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Created/Imported Tunnel Elements tab button.

5 Click on the Search button.

6 Perform one of the following actions to delete tunnel elements, as required:

- **a** Click on the Delete Unused button to delete tunnels that are no longer applied to a group. A dialog box appears.
- **b** Click on the Delete All button to delete all tunnels that are not associated with a service. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the elements and removes them from the list.

8 Close the rule properties form. The Manage Auto Tunnel Rules form reappears.

9 Close the Manage Auto Tunnel Rules form.

Procedure 52-8 To execute or reapply a topology rule

Use this procedure at any time after a rule is created. The execute button forces the topology rule to be evaluated; any missing or configuration changes are reapplied.

Note — The 5620 SAM supports the reapply function, except in reference to hop-less path changes. If a hop-less path changes, it may not be corrected by a reapply operation.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Select an auto tunnel rule type from the object drop-down menu.

3 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

4 Select a rule and click on the Properties button. The rule properties form opens.

5 Click on the More Actions button and choose Execute.

6 Close the Manage Auto Tunnel Rules form.

Procedure 52-9 To display missing tunnel elements

Perform this procedure to display the missing tunnel elements. A missing tunnel element is one that the 5620 SAM is unable to create based on the specified tunnel rules, or a tunnel element that is deleted.

1. Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.
2. Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.
3. Select a rule and click on the Properties button. The rule properties form is displayed.
4. Click on the Missing Tunnel Elements tab button.
5. Click on the Search button.
6. Select a missing tunnel element and click on the Properties button. The element properties form opens.
7. View the element properties.
8. Close the element properties form. The rule properties form reappears.
9. Close the rule properties form. The Manage Auto Tunnel Rules form reappears.
10. Close the Manage Auto Tunnel Rules form.

53 — RADIUS-based accounting policies

53.1 RADIUS-based accounting policies overview

A RADIUS-based accounting policy is used to send accounting information to a RADIUS server. The 7710 SR, 7450 ESS, and 7750 SR support the use of RADIUS-based accounting policies.

When a NE uses a RADIUS-based accounting policy and the creation of a subscriber host invokes the policy, the NE generates an accounting-start packet that includes the policy parameters, and forwards the packet to a RADIUS server. Depending on the policy specifications, the NE also sends interim update messages that contain usage statistics. When a policy is no longer used by any subscriber host, the NE sends an accounting-stop packet that contains the final usage statistics.

A RADIUS-based accounting policy specifies the type of accounting information that is forwarded to a RADIUS server. The information is one of the following:

- per-SLA profile—forwards start, stop, and interim update messages regarding SLA profile usage
- per-host and per-SLA profile—forwards the following:
    - start, stop, and interim update messages regarding SLA profile usage
    - start and stop messages for individual host sessions
- per-host only, on Release 9.0 and later NEs—forwards start, stop, and interim update messages for each subscriber host session

See chapter 68 for information about configuring RADIUS-based accounting policies for subscriber profiles.

53.2 RADIUS-based accounting policies procedures

The following procedures describe how to configure and manage RADIUS-based accounting policies.

Procedure 53-1 To configure RADIUS-based accounting policies

Perform the following procedure to create a RADIUS-based accounting policy to send subscriber session accounting information to the RADIUS server.

1 Choose Policies→RADIUS Based Accounting from the 5620 SAM main menu. The RADIUS Based Accounting Policies form opens.

2 Click on the Create button. The Radius Accounting Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Session ID Format
- Source Address
- Retry Attempts
- Timeout (seconds)
- Access Algorithm
- RADIUS Attributes
- Use Standard Accounting Attribute
- Host Accounting Message
- Enable
- Value (minutes)
- Port Prefix Type
- Port Prefix String
- Port Suffix Type
- Port Type
- Port Type Value
- Calling Station ID Type
- Port Binary Specification

Note — The Port Prefix Type Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the value of Port Type is set to Config.

The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Binary Specification parameter is configurable when the NAS Port option is enabled for the RADIUS Attributes parameter.

4 Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step 5. Otherwise, go to step 6

Note — The Router Instance parameter is configurable on the 7450 ESS, 7710 SR, and 7750 SR.

5 Configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy. Perform the following:

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Radius Accounting Policy list form opens.

ii Select a VPRN site in the list and click on the OK button. The Select VPRN ID - Radius Accounting Policy list form closes and the Radius Accounting Policy (Create) form refreshes with the VPRN service information.

6 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab button.

ii Click on the Create button. The RADIUS Server (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- Secret Name

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

vi Repeat steps ii and v to add additional RADIUS servers, as required.

7 Click on the OK button.

8 Perform the following steps.

i Click on the Custom Record tab button. The Significant Change Criteria tab is displayed.

ii Configure the Significant Change Delta parameters.

iii Configure the parameters in the Reference Queue panel:

Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Queues
- Ingress Counters
- Egress Counters

iv If the All Overrides parameter is enabled, go to step vii.

v Click on the Select button below the All Overrides parameter to choose a queue to monitor for the significant change. The Select Queue form opens.

vi Select a queue in the list and click on the OK button. The Select Queues form closes and the queue ID is displayed on the form.

vii Configure the parameters in the Reference Override panel:

Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Overrides
- Ingress Counters
- Ingress Counters

viii If you do not enable the All Overrides parameter, go to step 9.

ix Click on the Select button below the All Overrides parameter to choose an override counter to monitor for the significant change. The Select Override form opens.

x Select an override in the list and click on the OK button. The Select Override form closes and the override ID is displayed on the form.

9 Perform the following steps.

i Click on the Queue Counter Config tab button.

ii Click on the Create button. The CustomQueueConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

10 Perform the following steps.

i Click on the Override Counter Config tab button.

ii Click on the Create button. The CustomOverrideConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

11 Close the Radius Accounting Policy (Create) form. The Manage Radius Based Accounting Policies form reappears.

12 Click on the Search button to display the newly created policy or policies. Select a policy.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

14 Close the Manage Radius Based Accounting Policies form.

54 — 802.1x policies

54.1 802.1x policies overview

The 5620 SAM implementation of the 802.1X protocol provides 802.1X authentication on an individual port basis.

In an 802.1X environment, a user called the supplicant requests access to an access point, called the authenticator. The authenticator forces the supplicant into an unauthorized state, forcing them to send an EAP start message.

The authenticator returns an EAP message to request the user identity. The user returns the identity, which is forwarded by the authenticator to the authentication server. The server authenticates the user and returns an accept or reject message to the authenticator.

If an accept message is received, the authenticator changes the user state to authorized and user traffic is processed.

54.2 802.1x policies procedures

The following procedures describe how to configure and manage 802.1x policies.

Procedure 54-1 To configure an 802.1X policy

Note — Before you can create an 802.1X policy, 802.1X must be enabled on the device. See Procedure 17-6 for information about enabling 802.1X.

1 Choose Policies→Ethernet→802_1x from the 5620 SAM main menu. The Manage 802_1x Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 802_1x Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Source Address
- Administrative Status
- Description
- Retry Attempts
- Request Timeout

Note — Do not use a colon in the policy name. The 5620 SAM uses colons as separators for the object full name.

4 Click on the RADIUS Servers tab button, if required. Otherwise, go to step 8.

5 Click on the Create button. The RADIUS Server (Create) form opens.

6 Configure the parameters:

- Server Index
- IP Address
- Password
- Authorization Port
- Accounting Port
- Server Type

7 Click on the OK button. The Radius Server (Create) from closes and the 802_1x Policy (Edit) form refreshes with the server information displayed in the Radius Servers tab.

8 Click on the Apply button to save the policy. The 802_1x Policy form is refreshed with additional buttons and tab buttons.

9 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

10 Close the 802_1x Policies form.

11 Close the Manage 802_1x Policies form.

55 — PBB MRP policies

55.1 PBB MRP policies overview

This chapter describes how to configure and manage PBB MRP policies.

55.2 PBB MRP policies procedures

The following procedures describe how to configure and manage PBB MRP policies.

Procedure 55-1 To configure a PBB MRP policy

The PBB MRP policy limits the scope of MMRP advertisements to a specific network domain using ISID-based filters for both the MMRP control plane and the B-VPLS data plane. The policy contains a configurable option to instantiate an MMRP tree and related entry only when both an MMRP declaration and registration are received on a port.

1 Choose Policies→Ethernet→PBB MRP from the 5620 SAM main menu. The PBB MRP Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The PBB MRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Scope
- Default Action

4 Click on the Entries tab.

5 Click on the Create button to create entries for the policy. The PBB MRP Policy Entry (Create) form opens.

6 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Action

7 Click on the ISID Match Criteria tab.

8 Click on the Create button to specify ISID matching criteria for an entry in the policy. Multiple ISID matching criteria can be specified for each entry. The ISID Match Criteria (Create) form opens.

9 Configure the parameters:

- Low ISID
- High ISID

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ISID Match Criteria you specified appears in the list.

12 Perform one of the following:

a Add another set of criteria. Go to step 8.

b Click on the OK button. A dialog box appears.

13 Click on the OK button. The Entries tab reappears.

14 Click on the OK button. The Entries tab closes.

15 Close the PBB MRP Policy Manager form.

56 — AOS Ethernet Service policies

56.1 AOS Ethernet Service policies overview

This chapter describes how to configure the UNI and SAP profiles associated with OmniSwitch Ethernet services.

56.2 AOS Ethernet Service policies procedures

The following procedures describe how to configure AOS Ethernet Service policies.

Procedure 56-1 To configure an OmniSwitch Ethernet service UNI profile

1 Choose Policies→Ethernet→AOS Ethernet Service from the 5620 SAM main menu. The Manage Ethernet Service Policies form opens.

2 Perform one of the following:

  a Specify a filter to search for and modify an existing UNI profile. Select a profile in the filtered list and click on the Properties button.

  b Click on the Create button and choose Create UNI Profile. The Ethernet Service UNI Profile, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- STP
- GVRP
- 802.1x
- 802.3ad
- MVRP
- OAM
- UDLD
- VTP
- PVST
- UPLINK
- 802.1AB
- AMAP
- LACPMARKER
- PAGP
- CDP
- DTP
- VLAN
- Tunnel MAC

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Ethernet Service UNI Profile, Global Policy (Create) form closes.

5 To create more UNI profiles repeat steps 2b to 4.

6 Close the Manage Ethernet Service Policies form.

Procedure 56-2 To configure an OmniSwitch Ethernet SAP profile

1 Choose Policies→Ethernet→AOS Ethernet Service from the 5620 SAM main menu. The Manage Ethernet Service Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing SAP profile. Select a profile in the filtered list and click on the Properties button.

b Click on the Create button and choose Create SAP Profile. The Ethernet Service SAP Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Ingress Bandwidth (Mb)
- Bandwidth Sharing
- CVLAN Treatment
- Priority Mapping
- Priority

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Ethernet Service SAP Profile, Global Policy (Create) form closes.

5 To create more SAP profiles repeat steps 2b to 4.

6 Close the Manage Ethernet Service Policies form.

57 — Connection profile policies

57.1 Connection profile policies overview

The 5620 SAM implementation of the connection profile policy provides a list of VPI/VCI pairs.

57.2 Connection profile policies procedures

The following procedures describe how to configure and manage connection profile policies.

Procedure 57-1 To configure a connection profile policy

1 Choose Policies→ATM→Connection Profile from the 5620 SAM main menu. The Manage Connection Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify a policy, and click on the Properties button.

b Click on the Create button. The Connection Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Connection Profile ID
- Description

Note — Do not use a colon in the policy name. The 5620 SAM uses colons as separators for the object full name.

4 Click on the ATM Member tab button and click on the Create button. The ATM Member (Create) form opens.

5 Configure the parameters:

- VPI
- VCI

6 Click on the OK button. The ATM Member (Create) from closes and the Connection Profile (Edit) form refreshes with the VPI and VCI information displayed in the ATM Member tab.

7 Click on the Apply button to save the policy. The Connection Profile form is refreshed with additional buttons and tab buttons.

8 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices.

Note — When the policy is in draft mode, the Distribute option is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to local definitions. See chapter 46 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

9 Close the Connection Profile form.

10 Close the Manage Connection Profile form.

58 — Service PW template policies

58.1 Service PW template policies overview

Service PW templates are policies that enable PE routers to discover the other participating PE routers in an LDP or BGP VPLS.

58.2 Service PW template policies procedures

The following procedure describes how to configure service PW templates.

Procedure 58-1 To create or configure a PW Template policy

1 Choose Manage→Service→Service PW Template Policies from the 5620 SAM main menu. The Manage Service PW Template Policies form opens.

2 Perform one of the following:

a Click on the Create button. The Service PW Template (Create) form opens with the General tab displayed.

b Search for an existing policy you want to modify.

i Click on the Search button.

ii Select a policy from the displayed list.

iii Click on the Properties button. The Service PW Template (Edit) form opens with the General tab displayed.

3 Perform one of the following:

a Click on the More Actions button and choose Populate from Pseudowire.

This allows you to populate the Service PW Template form using an existing pseudowire (SDP Binding) as a base.

i After choosing Populate from Pseudowire, the Select a Pseudowire form opens.

ii Click on the Search button.

iii Choose the required pseudowire from the displayed list.

iv Click on OK. All of the relevant values are copied into the Service PW Template form.

v Go to step 19.

b Populate the form manually.

i Configure the following parameters:

- Policy ID
- Auto-Assign ID
- Description
- Enable Hash Label
- Enable Signal Capability
- Use Provisioned SDP
- Force VLAN VC Forwarding
- Enable Control Word
- VC Type
- Collect Stats

ii Select an Accounting Policy, if required, by clicking on the Select button. The Select Accounting Policy form opens.

iii Select an accounting policy and click OK, or create a new one by clicking on the Create button.

4 Click on the MAC tab button.

5 Configure the following parameters, as required:

- MAC Learning
- MAC Aging
- Discard Unknown Source
- Limit MAC Move
- MAC Pinning
- VLAN VC Tag
- MAC Address Limit

6 Click on the Split Horizon Group tab button.

7 Configure the following parameters, as required:

- Split Horizon Group Name
- Description
- Restrict Protected Source
- Restrict Unprotected Destination

8 Click on the Ingress Filters tab button.

9 Configure the Ingress Filter Type parameter, if required.

10 Click on the Egress Filters tab button.

11 Configure the Egress Filter Type parameter, if required.

12 Click on the IGMP tab button.

13 Configure the following parameters, as required:

- IGMP Version
- IGMP Fast Leave
- IGMP Import Policy
- IGMP Last Member Interval (deciseconds)
- IGMP Max Number Groups
- IGMP Max Number Sources Per Group
- IGMP General Query Interval (seconds)
- IGMP Query Response Interval (seconds)
- IGMP Robust Count
- IGMP Send Queries

14 If you need to re-configure an existing, distributed local PW Template, go to step 15. Otherwise go to step 19.

15 Click on the Local Definitions tab button.

16 Select the required entry from the list and click the Properties button. The Service PW Template - Local Policy - (Edit) form opens with the General tab displayed.

17 Make any required changes here - the tabbed pages are essentially the same as for the global definition of the PW Template covered in steps 3 through 13.

18 Click the More Actions button and choose Re-evaluate PW Template to run an evaluation of the modified template. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed. If you make any subsequent modifications, you can re-evaluate the template again.

19 Click on the OK button to confirm your changes. The Service PW Template - Local Policy - (Edit) form closes.

20 Click on the OK button to close the Service PW Template - Global Policy form.

59 — Residential subscriber policies

59.1 Residential subscriber policies overview

Residential subscriber management requires the use of policies and profiles that include the following:

- subscriber identification policies
- subscriber profiles
- SLA profiles

A subscriber identification policy is a component of residential subscriber management. It associates dynamic residential subscriber hosts with NE subscriber instances for the purpose of applying SLA profiles and subscriber profiles that act as templates for defining QoS, security and accounting attributes. There is no default subscriber identification policy in the 5620 SAM, but an operator can create a subscriber identification policy and designate it as the default.

A subscriber identification policy uses a parsing script to extract a subscriber identifier from a host DHCP packet. A common subscriber identifier indicates that hosts belong to the same subscriber and receive common HQoS and accounting treatment. A subscriber identification policy also assigns SLA profiles to hosts of a specific subscriber based on the type and class of service offering.

See chapter 68 for information about configuring and using subscriber identification policies, subscriber profiles, SLA profiles, and other residential subscriber management components.

60 — Remote network monitoring policies

60.1 Remote network monitoring policies overview

You can create remote network monitoring (RMON) policies that allow you to perform the following tasks.

- Use the policy framework to configure RMON that allows 5620 SAM users to deploy configurations to multiple devices.
- Map RMON events to information alarms in the 5620 SAM GUI.

Remote network monitoring allows you to monitor the behavior of functions that are not typically supported by the 5620 SAM. For example, events may be configured on generic NEs to monitor system temperature or CPU usage. The 5620 SAM can raise informational alarms for the exceeded thresholds. You can also configure custom values to supersede the hard-coded threshold values associated with a specific function on an NE.

The 5620 SAM maps RMON SNMP traps to alarms in the GUI.

Policy distribution and event mapping are supported for the following NE types:

- 7210 SAS-M24F
- 7210 SAS-M24F2XFP
- 7210 SAS-M24F2XFP [ETR]
- 7210 SAS-X24F2XFP
- 7250 SAS, Release 2.0 or later
- 7250 SAS-ES, Release 2.0 or later
- 7450 ESS
- 7710 SR
- 7750 SR

60.2 Remote network monitoring policies procedures

The following procedures describe how to configure and manage RMON policies.

Procedure 60-1 To configure a remote network monitoring policy

1. Choose Tools→Remote Network Monitoring (RMON) from the 5620 SAM main menu. The Remote Network Monitoring (RMON) form opens.

2. Perform one of the following:

   a. Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

   b. Click on the Create button. The RMON (Create) form opens.

3. Configure the parameters:

   - Displayed Name
   - Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Create events to associate with the rising and falling thresholds on the remote NE.

i Click on the Events tab button.

ii Click on the Create button. The Event RMON (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Type
- Owner
- Community

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Event RMON (Create) form closes and the RMON (Create) form reappears.

vi Repeat steps 4ii to v to create another event, if required.

5 Configure the alarm information that is associated with the remote event.

i Click on the Alarms tab button.

ii Click on the Create button. The Alarm RMON form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Monitored Object OID
- Interval (seconds)
- Sample Type
- Start Up Alarm
- Owner

6 Configure the properties for the rising threshold crossing alarm.

i Click on the Select button in the Rising TCA Properties panel. The Select Rising Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Rising Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Rising Threshold parameter.

7 Configure the properties for the falling threshold crossing alarm.

i Click on the Select button in the Falling TCA Properties panel. The Select Falling Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Falling Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Falling Threshold parameter.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Alarm RMON form closes and the RMON (Create) form reappears.

10 Click on the Apply button.

11 Click on the More Actions button and choose Distribute to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

> **Note —** When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

12 Close the RMON (Create) form. The Remote Network Monitoring (RMON) form reappears.

13 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

14 Close the Remote Network Monitoring (RMON) form.

61 — Size constraint policies

61.1 Size constraint policies overview

Size constraint policies regulate the number of historical records that the 5620 SAM database retains. The scheduling of tasks through the 5620 SAM can generate a great deal of archived result information if left unchecked. Size constraint policies control this volume by defining thresholds for various record classes. When the number of records for a specific class or group of classes reaches a threshold specified in the policy, the 5620 SAM deletes a specified number of the oldest objects that are associated with the class or group of classes.

61.2 Size constraint policies procedures

The following procedures describe how to configure and manage size constraint policies.

Procedure 61-1 To configure a size constraint policy

1 Choose Administration→Size Constraint from the 5620 SAM main menu. The Size Constraint Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Size Constraint Policy (Create) form opens.

3 Configure the parameters:

- Auto-Assign ID
- Policy Id
- Description
- Threshold (# of objects)
- Objects To Be Deleted When Threshold Exceeded (# of objects)
- Apply Threshold To

4 Click on the Constrained Packages tab button.

5 Right-click on the Size Constraint Policy icon and choose Select Packages from the contextual menu. The Select Size Constrained Packages form opens with a list of packages displayed.

6 Choose the packages to include in the size constraint policy and click on the OK button. The packages appear in the navigation tree under Constrained Packages.

7 From a package icon below the Size Constraint Policy icon, choose Select Classes from the right-click contextual menu to include in the size constraint policy.

i Right-click on a package and choose Select Classes from the contextual menu. The Select Size Constrained Classes form opens.

ii Choose the required classes in the list and click on the OK button. The classes appear in the navigation tree under the associated package.

8 Repeat step 7 for each package icon in the list.

9 Click on the OK button. The Size Constraint Policy Manager form reappears with the new size constraint policy displayed in the list.

10 Close the Size Constraint Policy Manager form.

62 — NAT policies

62.1 NAT policies overview

A Network Address Translation, or NAT, policy, defines general NAT properties and associates a NAT address pool with an ISA-NAT group on the same NE. A NAT policy is associated with a subscriber profile for L2-aware NAT in an IES or VPRN service, or for large-scale NAT in a VPRN service.

See chapter 18 for information about ISA-NAT groups. See chapter 30 for information about configuring and deploying NAT in a network. See Procedure 62-1 for NAT policy configuration information. See chapter 73 for information about configuring and using NAT in an IES. See chapter 74 for information about configuring and using NAT in a VPRN service.

62.2 NAT policies procedures

The following procedures describe how to configure and manage NAT policies.

Procedure 62-1 To create a NAT policy

Perform this procedure to create a NAT policy for a large-scale or L2-aware NAT implementation.

1. Choose Policies→ISA Policies→NAT Policy from the 5620 SAM main menu. The NAT Policy Manager form opens.

2. Click on the Create button. The NAT Policy (Create) form opens.

3. Configure the following parameters:
   - Displayed Name
   - Description

4. Click on the Select button in the NAT Pool panel to choose a NAT pool. The Select NAT Pool form opens.

5. Choose a NAT pool in the list and click on the OK button. The Select NAT Pool form closes and the NAT pool name is displayed on the NAT Policy (Create) form.

6. Configure the remaining parameters:
   - Filtering
   - Port Reservation Count
   - High Watermark
   - Low Watermark
   - Session Limit
   - Reservation Count
   - Session High Watermark
   - Session Low Watermark
   - ALG Protocols
   - UDP Inbound Refresh
   - Priority Session Forwarding Class Set
   - TCP Established (sec)
   - TCP Transitory (sec)
   - TCP Syn (sec)
   - TCP Time Wait (sec)
   - ICMP Query (sec)
   - UDP (sec)
   - UDP Initial (sec)
   - UDP DNS (sec)
   - SIP (sec)

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The NAT Policy (Create) form closes.

9 Close the NAT Policy Manager form.

63 — Format and range policies

63.1 Format and range policies overview

The 5620 SAM supports format and range policies. Format policies manage how services, policies, LSPs, L2 and L3 access interfaces are named and described. Range policies manage the ID numbers that are assigned to services, policies, LSPs, L2 and L3 access interfaces. For example, you can configure a range policy to specify a range of 200 and 499 for all IDs for a service. You can configure a format policy to specify that service names do not exceed 10 characters. The object creation form indicates when a range or format policy is in effect for an object.

Format and range policies are not distributed to NEs. The format and range policies are configured when services, policies, LSPs, L2 and L3 access interfaces are created from the 5620 SAM GUI. You cannot configure format and range policies when the services, LSPs, L2 and L3 access interfaces are created using templates. However, the 5620 SAM allows an operator to use pre-configured examples of LSPs and services that have format and range policies applied to them. The examples can be used to create a template. For more information about creating templates from a pre-configured example, see the *5620 SAM Scripts and Templates Developer Guide*.

Table 63-1 lists the objects and associated parameters that can be managed using format and range policies.

Table 63-1 Format and Range policy objects and associated parameters

Object name	Format policy parameter	Range policy parameter
B-VPLS Service Site	Description, Name	—
Bypass-only LSP	Description, Name	ID
Customer	—	ID
Dynamic LSP	Description, Name	ID
I-VPLS Service Site	Description, Name	—
IES Group Interface	Description, Name	Interface ID
IES L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
IES Service	Description, Service Name	Service ID
IES Service Access Point	Description, Name	Outer Encapsulation Value
IES Service Site	Description, Name	—
IES Subscriber Interface	Description, Name	Interface ID
IP Mirror Interface	—	Interface ID
MVPLS B-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS I-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS L2 Access Interface	Description	Outer Encapsulation Value
MVPLS Service	Description, Service Name	Service ID
Mirror L2 Access Interface	—	Outer Encapsulation Value
MVPLS Service B-Site	Description, Name	—
MVPLS Service I-Site	Description, Name	—

(1 of 2)

Object name	Format policy parameter	Range policy parameter
MVPLS Service Site	Description, Name	—
Mirror Service	Description, Service Name	Service ID
Mirror Service Site	Description, Name	—
Redundant Interface	—	Interface ID
Spoke SDP Binding	—	VC ID
Static LSP	Description, Name	ID
Tunnel	Description, Name	ID
VLAN L2 Access Interface	Description	—
VLAN Service	Description, Service Name	Service ID
VLAN Service Access Point	Description, Name	—
VLAN Service Site	Description, Name	—
VLL Apipe Service	Description, Service Name	Service ID
VLL Apipe Service Site	Description, Name	—
VLL Cpipe Service	Description, Service Name	Service ID
VLL Cpipe Site	Description, Name	—
VLL Epipe Service	Description, Service Name	Service ID
VLL Epipe Service Site	Description, Name	—
VLL Fpipe Service	Description, Service Name	Service ID
VLL Fpipe Service Site	Description, Name	—
VLL Ipipe L2 Access Interface	Description	Outer Encapsulation Value
VLL Ipipe Service	Description	Service ID
VLL Ipipe Site	Description, Name	—
VLL L2 Access Interface	Description	Outer Encapsulation Value
VPLS B-L2 Access Interface	Description	Outer Encapsulation Value
VPLS I-L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Management Interface	—	Interface ID
VPLS Service	Description, Service Name	Service ID
VPLS Service Site	Description, Name	—
VPRN Group Interface	Description, Name	Interface ID
VPRN L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
VPRN Service	Description, Service Name	Service ID
VPRN Service Access Point	Description, Name	Outer Encapsulation Value
VPRN Service Site	Description, Name	—
VPRN Subscriber Interface	Description, Name	Interface ID

(2 of 2)

Table 63-2 lists the policies that support format and range policies.

Table 63-2 Format and Range policy objects and associated parameters for policies

Policy	Format policy	Range policy
Access Ingress QoS	Description, Displayed Name	ID
Access Egress QoS	Description, Displayed Name	ID
ATM QoS policy	Description, Displayed Name	ID
Egress Queue Group template	Description, Displayed Name	—
7705 SAR Fabric Profile	Description, Displayed Name	ID
Policer Control policy	Description, Displayed Name	—
HSMDA Pool policy	Description, Displayed Name	—
HSMDA Scheduler policy	Description, Displayed Name	—
HSMDA WRED Slope policy	Description, Displayed Name	—
Ingress Queue Group template	Description, Displayed Name	—
MCFR Egress QoS Profile	Description	Profile ID
MCFR Ingress QoS Profile	Description	Profile ID
MLPPP Egress QoS Profile	Description	Profile ID
MLPPP Ingress QoS Profile	Description	Profile ID
Named Buffer Pool policy	Description, Name	—
Network policy	Description, Displayed Name	ID
Network Queue	Description, Name	—
Port Scheduler policy	Description, Displayed Name	—
Sap Access Ingress for 7210	Description, Displayed Name	ID
Network Policy for 7210	Description, Displayed Name	NW Mgr ID, Policy Id
Network Queue for 7210	Description, Name	—
Port Access Egress for 7210	Description, Displayed Name	ID
Port Scheduler for 7210	Description, Displayed Name	—
Slope Policy for 7210	Description, Displayed Name	—
Scheduler policy	Description, Displayed Name	—
WRED Slope policy	Description, Displayed Name	—
ACL IP filter	Description, Displayed Name	Filter ID
ACL IPv6 filter	Description, Displayed Name	Filter ID
ACL MAC filter	Description, Displayed Name	Filter ID
ANCP policy	Displayed Name	—
Host Tracking policy	Description, Displayed Name	—
MSAP policy	Description, Displayed Name	—
PPPoE policy	Description, Displayed Name	—
SLA Profile	Description, Displayed Name	—
Subscriber Explicit Map Entry	Description, Displayed Name	—

(1 of 2)

Policy	Format policy	Range policy
Subscriber Identification policy	Description, Displayed Name	—
Subscriber Profile	Description, Displayed Name	—
AA Application filter	—	Entry ID
Egress Multicast Group	Description, Displayed Name	—
Multicast Package	Description, Displayed Name	ID
Multicast CAC	Description, Name	—
Multicast PathMgmt BW policy	Description, Name	—
Multicast PathMgmt Info policy	Description, Name	—
AS Path	Description, AS Path Name	—
Community	Description, Community Name	—
Damping	Damping Name	—
Prefix List	Description, Prefix List Name	—
Statement	Description, Statement Name	—
MPLS Adminstrative Groups	Displayed Name	Value
Static Configuration for SRLGs	Displayed Name	—
Shared Risk Link Group Static Config	Displayed Name	Value
Accounting policy	Description, Displayed Name	ID
File policy	Description, Displayed Name	ID
Maintenance Domain	Description, Name	MD Mgr ID
Network Address Translation policy	Description, Displayed Name	—
PAE 802_1x policy	Description, Displayed Name	—
RADIUS Based Accounting	Description, Displayed Name	—
RMON	Description, Displayed Name	—
Time of Day Suite	Description, Name	—
Time Range	Description, Name	—
VRRP policy	Description, Displayed Name	ID, Service ID

(2 of 2)

63.2 Format and range policies procedures

The following procedures describe how to configure and manage format and range policies.

Procedure 63-1 To create or configure a format policy

Use this policy to specify the number and format of characters that can be used for text fields such as service names and descriptions.

1 Choose Administration→Format and Range from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Rules). A navigation tree is displayed.

3 Click on Format Policy (Property Rules).

4 Perform one of the following:

a Click on the Search button to specify a filter to search for and modify a policy. A list of format policies is displayed. Go to step 5.

b Click on the Create button. The Format Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a format policy in the list. A Format Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the name format policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Format Policy (Create) or (Edit) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens with a list of configurable properties for the object. The content of the list depends on the object that you specified in step 8.

11 Choose the property for which you need to apply the format policy.

12 Click on the OK button. The Select Property - Format/Range Policy form closes and Format Policy form is updated with property name.

13 Click on the Users tab button.

Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more format policies to a user or user group. See procedures 9-17 and 9-18 for more information about creating users and user groups.

14 Click on the Add button. The Select User form opens with a list of users.

15 Select one or more users in the list and click on the OK button. The Format Policy form is refreshed with the selected users.

16 Click on the User Groups tab button.

17 Click on the Add button. The Select Group form opens with a list of user groups.

18 Choose one or more user groups in the list and click on the OK button. The Format Policy (Create) or (Edit) form is refreshed with the selected user groups.

19 Click on the Text Block Formats tab button to further define the format of the text. For example, an operator can classify a group of services with a similar name. The operator can also create a tool tip text to describe the purpose of the parameter.

20 Click on the Move Up or Move Down buttons to change the sequence of the text blocks in the text string.

21 Click on the Create button and perform one of the following:

a Choose Auto-Filled Parameter. The Auto-Filled Parameter (Create) form opens.

b Choose Masked Text Parameter. The Formatted Text (Create) form opens. Go to step 24.

c Choose Text Parameter. The Text (Create) form opens. Go to step 26.

22 Configure the parameters:

- Source Object Name
- Source Property Name
- Copy Text From Position
- Through To Position
- Displayed Text
- Tooltip Text

23 Go to step 27.

24 Configure the parameters:

- Mask
- Tooltip Text

25 Go to step 27.

26 Configure the parameters:

- Default Value
- Read Only
- Min. Length
- Max. Length
- Tooltip Text

Note — The Min. Length and Max. Length parameters are not configurable when the Read Only parameter is enabled.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The Format Policy form reappears.

29 Click on the OK button. The Format Policy form closes.

30 Close the Format and Range Policies form.

Note — After a format policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

Procedure 63-2 To create or configure a range policy

Use this policy to specify the ID range for services, LSPs, L2 and L3 access interfaces.

1 Choose Administration→Format and Range from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Values). A navigation tree is displayed.

3 Choose Range Policy (Property Rules).

4 Perform one of the following:

- **a** Click on the Search button to specify a filter to search for and modify a policy. A list of range policies is displayed. Go to step 5.
- **b** Click on the Create button. The Range Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a range policy in the list. A Range Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State
- Minimum
- Maximum
- Auto Assignment Enabled
- Auto Assign By Default

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the range policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Range Policy (Create) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens.

11 Choose the property for which you need to apply the range policy.

12 Click on the OK button. The Select Property - Format/Range Policy form closes and Range Policy (Create) form is updated with the property name.

13 Click on the Users tab button.

Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more range policies to a user or user group. See procedures 9-17 and 9-18 for more information about creating users and user groups.

14 Click on the Add button. The Select User form opens with a list of users.

15 Choose one or more users in the list and click on the OK button. The Range Policy form is refreshed with the users.

16 Click on the User Groups tab button.

17 Click on the Add button. The Select Group form opens with a list of user groups.

18 Choose one or more user groups in the list and click on the OK button. The Range Policy form is refreshed with the user groups.

19 Click on the OK button. The Range Policy form closes and the Format and Range Policies form reappears.

20 Close the Format and Range form.

Note — After a range policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a range policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

Service management

64 — Service management and QoS

64.1 Service management and QoS overview

The 5620 SAM supports the configuration of the following network services:

- VLL service
- VPLS / MVPLS / HVPLS
- IES
- VPRN service
- VLAN service
- composite service
- mirror service

A 5620 SAM operator can create, configure and delete services on sites and routers that are within their span of control.

The benefits of the 5620 SAM service model include:

- service creation using configuration forms or preconfigured XML API template; see the *5620 SAM Scripts and Templates Developer Guide* for information about creating and using XML API templates
- service management using configuration forms and a navigation tree
- linking of services to create composite services that support complex customer applications
- policies that specify the NE traffic classification, policing, shaping, time of day restrictions, and marking
- traffic management capabilities to customize the delivery of different services according to SLAs
- integrated fault management functions

Customer traffic enters a service through one or more access interfaces. In a local service, all access interfaces are on one NE. In a distributed service, multiple NEs are deployed at the PE. Customer traffic is transported across an IP/MPLS core network in unidirectional service tunnels that use GRE or MPLS LSPs. Many services can use the same tunnel. Figure 64-1 shows an example of a distributed VLL service.

Figure 64-1 Distributed VLL service

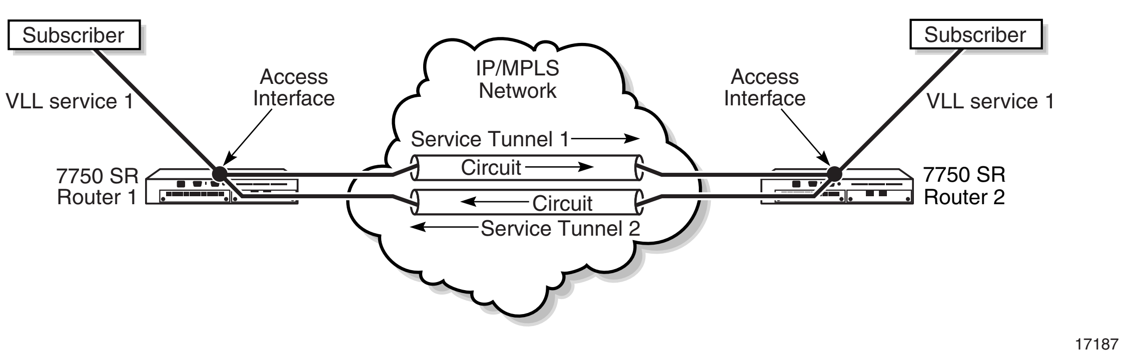
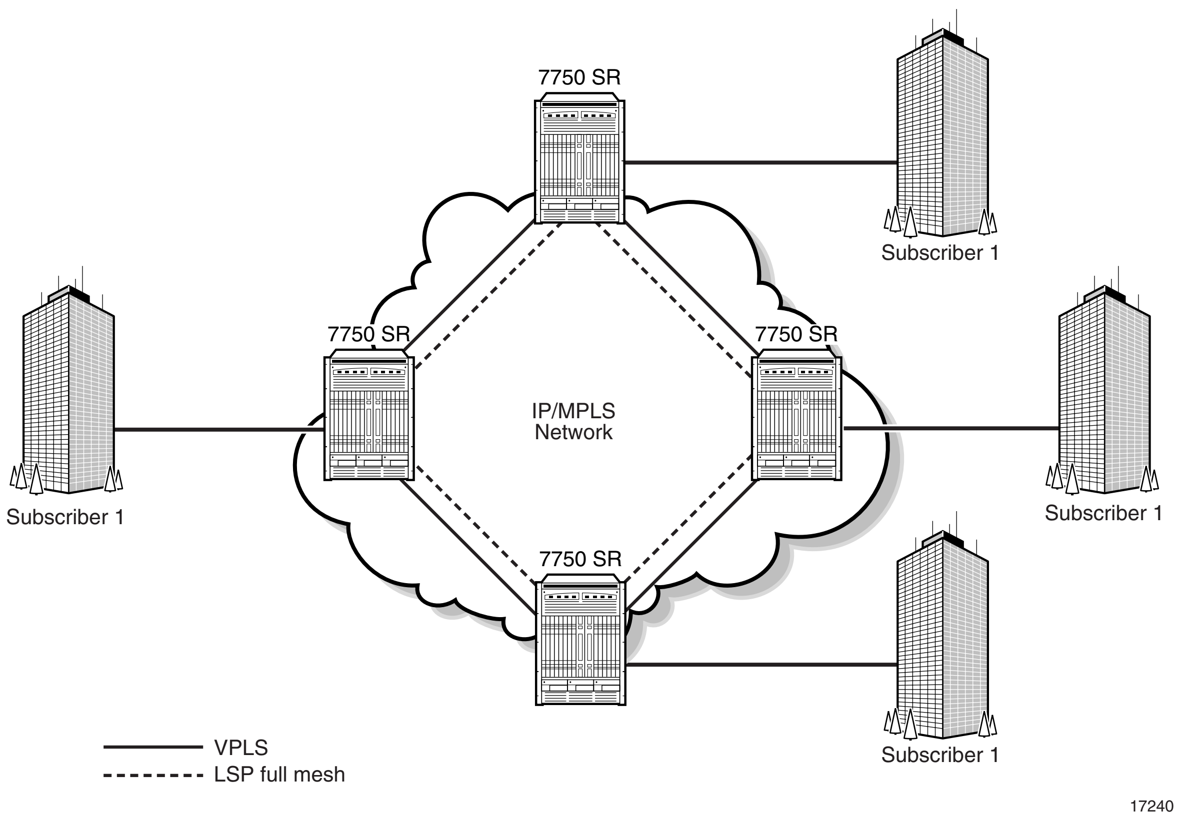


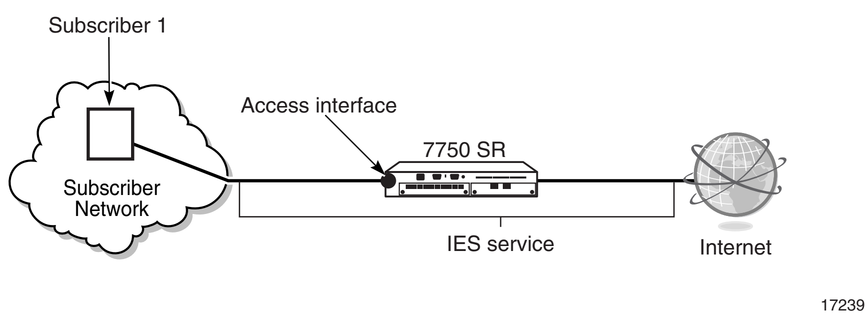
Figure 64-2 shows an example of a distributed VPLS.

Figure 64-2 Distributed VPLS



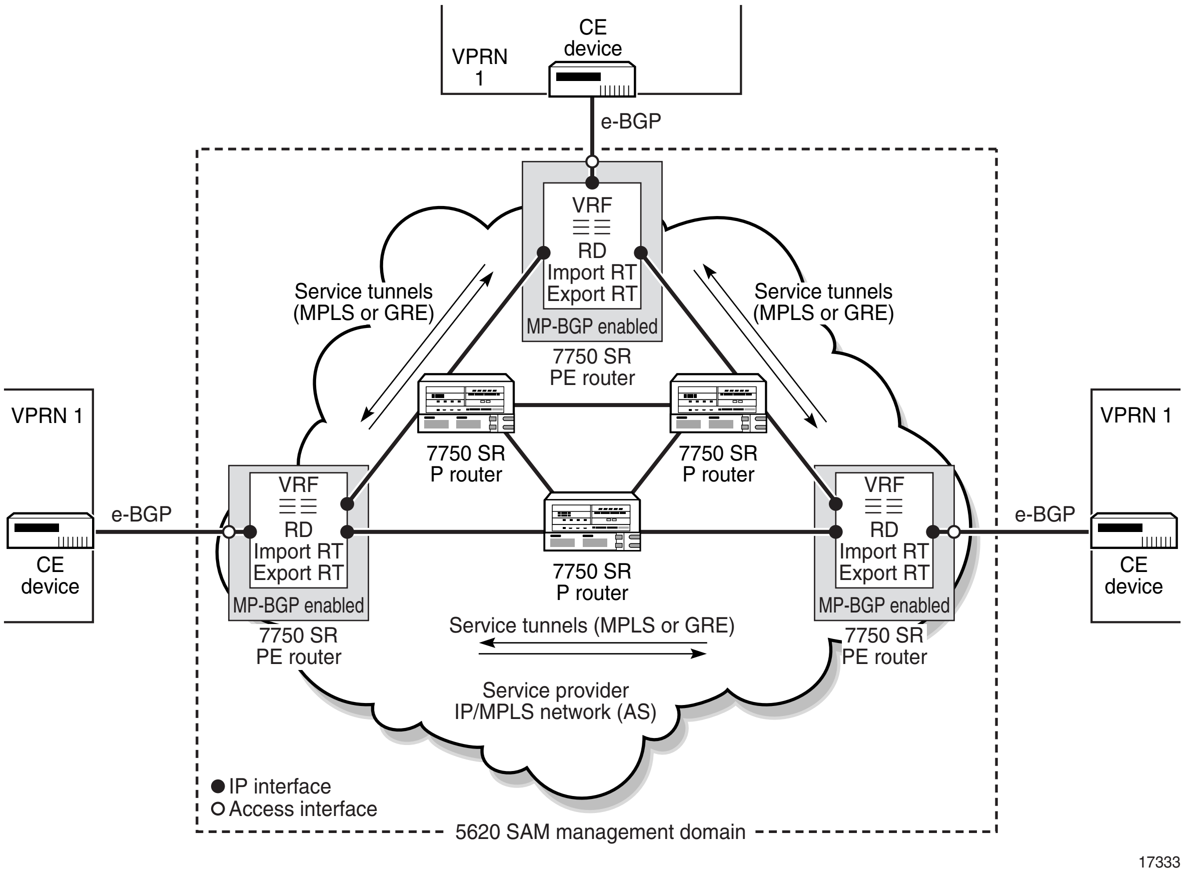
For IES, the managed devices are deployed at the provider edge and customer traffic enters the service using access interfaces. IES is a routed connectivity service where the customer communicates with an IP router interface to send and receive Internet traffic. Figure 64-3 shows a sample IES.

Figure 64-3 Sample IES



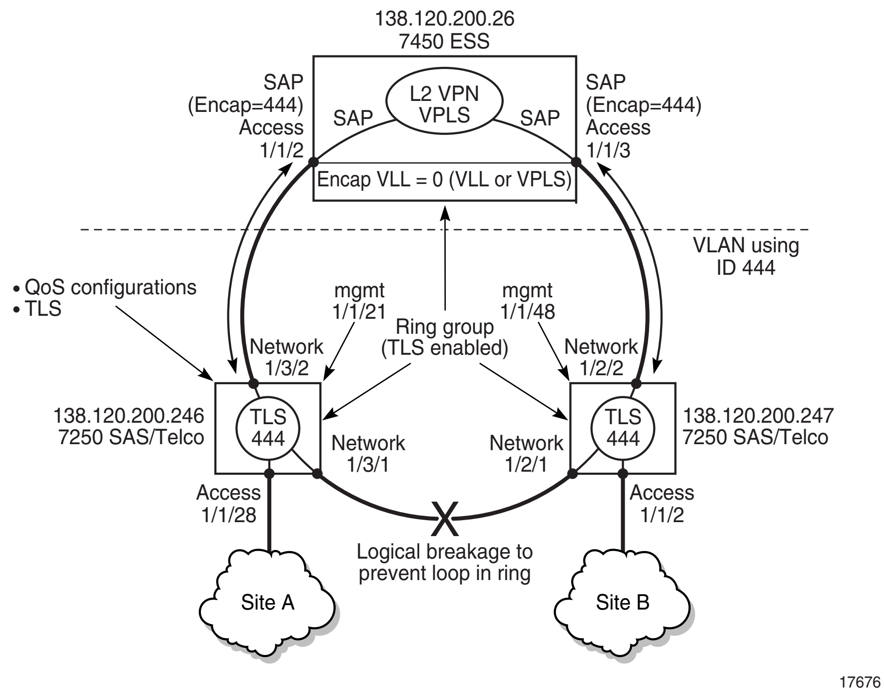
For VPRN services, the managed devices can be deployed as PE or provider core routers. Data and distribution of routing information are forwarded across an IP/MPLS service provider core network. Figure 64-4 shows a sample VPRN service.

Figure 64-4 Sample VPRN service



VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, a 7450 ESS, to all devices in the ring. STP configuration on 7250 SAS and Telco devices ensures that there is a constant stream of traffic in either direction. Any breaks in the physical links between devices are rerouted. Figure 64-5 shows a sample VLAN for L2 VPNs.

Figure 64-5 Sample VLAN configuration for L2 VPNs



A composite service allows the interconnection of different service types to form a service delivery network that is tailored to a specific application. For example, VPRN, VPLS, and VLAN services can be joined to create a routed multicast TV distribution mechanism that spans a wide geographical area.

A mirror service is a unidirectional service function that duplicates a specified traffic stream and sends the duplicate stream to a monitoring device for troubleshooting or surveillance purposes. With pseudo-wire redundancy support, an ICB can be enabled in a mirror service spoke and a remote source, which can provide bidirectional service that enables support for active and standby PE redundancy.

QoS provides the ability to rate limit across multiple queues from one or more access interfaces for a customer, and to differentiate service levels for different types of traffic. For higher priority traffic such as VoIP or video, you can specify reserved bandwidth. Lower priority applications, such as data traffic, may not have reserved bandwidth but can burst to use all the available bandwidth.

The main elements of QoS are:

- QoS markings

  Customer traffic may be marked with QoS markings, such as DSCP, EXP, and dot1p, that are mapped to forwarding classes.

  All forwarding classes support profile marking of packets as in-profile or out-of-profile. In-profile packets have a high enqueuing priority. Out-of-profile packets have a low enqueuing priority. Profile marking of packets can occur at two points: when packets are classified into forwarding classes at access ingress and when packets are classified at service egress. Profile marking is only done on the internal header and not in an actual encapsulation.

- forwarding classes

  Provide network elements with a method to weigh the relative importance of packets, only in relation to other forwarding classes. A forwarding class is also referred to as a Class of Service.
- queues

  Location for buffering packets that are to be forwarded before they are scheduled.
- schedulers

  Hardware scheduling (or single-tier scheduling) exists by default on a device and consists of a high-priority and a low-priority scheduler.

  Scheduler policies (or multi-tier scheduling) provide a more complex, hierarchical structure of virtual schedulers that override the default hardware behavior for more flexible scheduling capabilities.
- slope policies

  Define the WRED slope characteristics of hardware buffer space that is used by the ingress and egress queues

See chapter 46 for more information about policies on the 5620 SAM. See the *7750 SR OS Services Guide* for more detailed information about QoS.

Access interfaces

Each customer service is configured with at least one access interface point called a SAP. The access interface identifies the point of customer interface for a service on the managed device.

A Layer 2 or Layer 3 access interface is uniquely identified using these parameters:

- physical Ethernet port or POS port and channel
- encapsulation type (if applicable)
- encapsulation id (if applicable)

Depending on the encapsulation type, a physical port or channel can have more than one access interface associated with it. Using encapsulation or a SONET/SDH channel, devices can support multiple services for a customer or for multiple customers.

Access interfaces can only be created on ports or channels that are designated as access in the physical port configuration. Access interfaces cannot be created on ports designated as core-facing network ports because these ports have a different set of features enabled in software.

Access interfaces can participate in policies. Time of day suites can also be associated with access interfaces to apply a set of time-based policies, filters, and schedulers. Configuration of access interfaces can be performed during service configuration or modification. When you configure an access interface, consider the following:

- An access interface is owned by and associated with the service in which it is created.
- An access interface is a local entity and is locally unique to a specific device. The same access interface ID value can be used on another device.
- There are no default access interfaces. All access interfaces must be created.

- The default administrative state for an access interface at creation time is administratively enabled.
- If a port or channel is shut down (administratively or operationally), access interfaces on that port/channel are operationally out of service.

Automatic SDP (service tunnel) binding for services

You configure automatic service tunnel (SDP) binding for services when you configure a service using configuration forms or templates.

The 5620 SAM defines its own internal rules on how automatic mesh SDP bindings are performed.

1. The 5620 SAM tries to find the least-used SDP (service tunnel) with the lowest load factor (the lower the number of bindings, the lower the load factor) from the source to destination node when the service tunnel meets the following conditions:
   - the service tunnel operational state is up
   - the operational MTU is greater than or equal to the MTU value of the service site
   - T-LDP is set for SDP bindings of VPLS, IES, or VLL services
   - the selected transport method, either GRE, LDP, or RSVP
2. When no service tunnel operational state is up, 5620 SAM tries to find the least-used service tunnel with the lowest load factor in an operationally down state.
3. For mirror services, binding are created from the source sites to the destination sites.
4. When a service tunnel cannot be found for a service site, a change in the site leads to another search. For example, if the service MTU is 1500 and the highest path MTU in all SDPs from that site is 1472, no SDP binding can be successful. If the service MTU is lowered to 1472 or less, a successful SDP binding results.
5. When a service tunnel is not found, and the transport method selected is GRE, 5620 SAM attempts to create a GRE service tunnel with a path MTU equal to the service site service MTU with T-LDP signaling turned on.

See “MTU size and port configuration” in section 20.2 for more information on MTU size considerations.

Multi-segment tunnel selection

Multi-segment tunnel selection functionality enhances tunnel selection functionality to allow the system to select intermediate NEs in a path, as well as the service tunnels from a selected intermediate NE to its next hop. Multi-segment tunnel selection functionality is used to select existing SDPs. It cannot create new SDPs.

Tunnels are selected based on the following criteria:

- If a metric value is specified for any of the SDPs along the path, the path with the lowest sum of the metric property for all SDPs along the path is selected.
- If no metric is specified for any of the SDPs along the path, the path with the fewest number of SDPs (hops) is selected.
- If two paths or SDPs are equal based on the selection criteria mentioned above, the SDP/path with the lowest load factor (number of services using that SDP) is selected.

Multi-segment tunnel selection functionality must be enabled at the system level, as well as at the tunnel selection profile level. Table 64-1 describes the objects to which a tunnel selection profile with multi-segment tunnel selection can be assigned, and the service tunnel configurations that result.

Table 64-1 Multi-segment tunnel selection scenarios

Tunnel selection profile applied to...	Resulting tunnel configuration
Spoke SDP binding on a VLL service	This scenario applies to a VLL service with two terminating sites. One of the sites has a spoke SDP binding configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites are created.
VLL service	This scenario applies to a VLL service with two terminating sites. The service is configured with Automatic SDP Binding/PBB Tunnel Creation enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites are created.
Spoke termination point	This scenario applies to a spoke SDP binding between any two supporting objects. These include (M-)VPLS sites, (M-)VPLS I-sites, (M-)VPLS B-sites, VLL sites, IES L3 access interfaces, VPRN L3 access interfaces, VLL endpoints, and VPLS endpoints. The spoke SDP binding is configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection enabled. If a termination point is specified, the spoke SDP bindings and return spoke SDP bindings are created. Switching sites are created as follows: • If the spoke SDP binding is created on a VLL service, the switching sites are created on the VLL service. • If the specified termination point is on a VLL service, the switching sites are created on the VLL service. • If neither end of the tunnel is on a VLL service, a new EPIPE service is created. The service component ID is auto-selected by the system. The subscriber ID is the same as the service on which the spoke is created. All other parameters are default values.

Redundant path selection

If Redundant Path Selection is enabled on a tunnel selection profile, a redundant path is created. Redundant Path Selection can only be enabled if Multi-Segment Tunnel Selection is also enabled. The selected redundant path does not use any of the same switching sites as the primary path. Redundant path selection is not supported when a termination point is selected on a spoke SDP binding. Table 64-2 describes the objects to which a tunnel selection profile with redundant path selection can be assigned, and the service tunnel configurations that result.

Table 64-2 Redundant path selection scenarios

Tunnel selection profile applied to...	Resulting redundant path configuration
Spoke SDP binding on a VLL service	This scenario applies to a VLL service with two terminating sites. One of the sites has a spoke SDP binding configured with Auto-Select Transport Tunnel enabled, and a tunnel selection profile with Multi-segment Tunnel Selection and Redundant Path Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites for the redundant path are created. In this case, an endpoint and a return endpoint must be specified.
VLL service	This scenario applies to a VLL service with two terminating sites. The service is configured with Automatic SDP Binding/PBB Tunnel Creation enabled, and a tunnel selection profile with Multi-segment Tunnel Selection and Redundant Path Selection enabled. If a valid path is found between the two terminating sites, the spoke SDP bindings and switching sites for the redundant path are created. From a VLL Service, endpoints on the terminating sites that do not have SAPs or spokes are used for the auto-created spokes. If multiple endpoints exist on a terminating site, the endpoint without any SAPs is used. If multiple viable endpoints are available, an error is raised by the 5620 SAM and the operation fails. If there are no endpoints available, an endpoint is automatically created with default parameter values, with the following exceptions: • The Name parameter value is the endpoint Service ID. • The Description parameter value is auto-generated by the system.

SDP binding template handling

Multi-segment tunnel selection functionality will use SDP binding templates to create spoke SDP bindings in cases where a template is specified. SDP binding templates are handled using the following logic:

1. If an SDP binding template is specified on a tunnel selection profile, the template is used when creating the spoke SDP bindings.
2. If the site on which an SDP binding is being created has an associated site template, then the system attempts to find an SDP binding template within the site template. If an SDP binding template is found, it is used to auto-create the

spoke SDP bindings. If two or more templates are found, the system creates a spoke SDP binding with default parameters. If no templates are found, the logic described in item 3 applies.

3 If a service is associated with a template, then an attempt is made to find an SDP binding template within that template. If an SDP binding template is found, it is used to auto-create the spoke SDP bindings. If no templates are found, or two or more templates are found, then the system creates a spoke SDP binding with default parameters.

Automatic PBB tunnel binding

This feature is applicable only to VLL Epipes and I-VPLS services using a PBB tunnel.

Note — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for more information about the availability of this feature.

The configuration of the service CAC functionality allows you to manage bandwidth at the service level and at the link level, which in turn enables the 5620 SAM to automatically select the best tunnel based on the number of active links and on the amount of available bandwidth on the service. The 5620 SAM also considers the shortest available path when it allocates bandwidth.

Although the 5620 SAM can select tunnels automatically—see Automatic SDP (service tunnel) binding for services—if service CAC is not configured, bandwidth will not be considered by the 5620 SAM when selecting the tunnel.

Bandwidth availability for the tunnel is calculated at the service admission request time and is based on the links currently used by the tunnel forwarding path. The booking of reserved bandwidth by the service is done directly on the link and directly on the tunnel, for a bandwidth-reserved tunnel.

The link monitors the bandwidth used by all of the services using that link. Since the bandwidth reserved on each tunnel that is used by a service can be different, the link monitors bandwidth usage through the tunnels rather than through a service.

You can perform a system-wide audit to ensure that the bandwidth on each link is properly calculated. The audit visits all tunnels in the network and adjusts the available bandwidth in all links currently being used by the forwarding tunnel path. The adjustments are made based on total bandwidth requests per CoS for all EVPLs currently using the tunnels.

You can perform this audit by clicking on the More Actions button on the Manage Services form and choosing CAC Audit. The audit also occurs automatically on system startup and when service CAC is switched from disabled to enabled. See chapter 6 for information about enabling and disabling service CAC.

Lightweight SAPs

SAPs that are associated with residential split horizon groups on VPLS sites are called lightweight SAPs. An RSHG uses dual-pass queue optimization and does not support downstream broadcast or multicast traffic. Lightweight SAPs have fewer internal configuration settings than regular SAPs. Therefore, you can create more lightweight SAPs on a node. The SAP Lightweight property is automatically set at creation time, when the SAP is associated with an RSHG, and cannot be modified later.

Users can:

- assign SAPs to residential split horizon groups
- list lightweight SAPs using the Lightweight filter property

Note — To get the most recent state of a lightweight SAP, it is recommended that users perform a resynchronization by clicking on the More Actions button and choosing Resync in the SAP configuration window.

64.2 5620 SAM and the triple play service delivery architecture

The TPSDA is based on three major components, as shown in Figure 64-6:

- broadband service aggregator
- broadband service router
- service and policy activation

Figure 64-6 TPSDA components

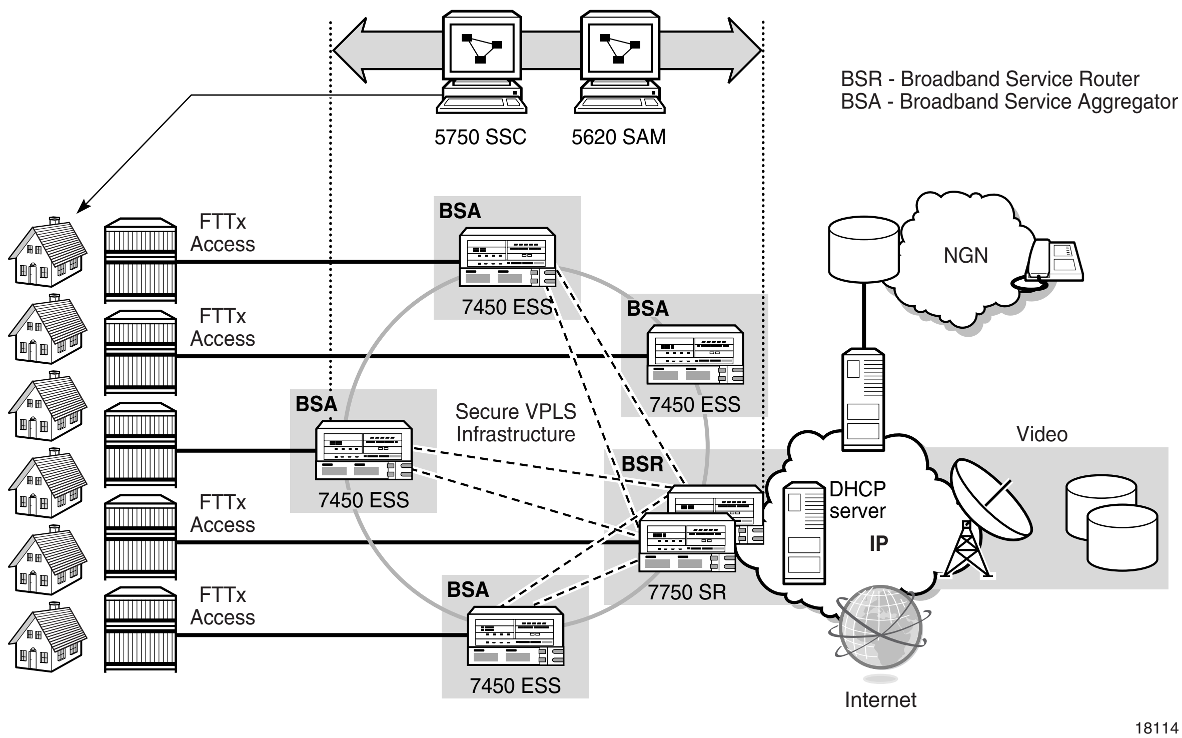


Table 64-3 lists the Alcatel-Lucent TPSDA product components.

Table 64-3 Product components of the TPSDA

Product	Role	Notes
5620 SAM	Provides network, service, and policy management across the TPSDA architecture, including a unified interface for element management and simple service activation and monitoring.	Create and configure QoS, filtering, and accounting templates that can then be reapplied to multiple L2 and L3 interfaces, and configure managed BSA and BSR devices to allow DHCP relay.
5750 SSC	Provides centralized control of host access services for triple play service delivery, for example, as a DHCP server to identify hosts and trigger service configuration or on-demand service profile changes made by the customer. Interworks with the 5620 SAM to enable per-customer QoS and bandwidth changes in the network.	Provide a customer self-service web portal and manage information that determines the levels of service allowed for an end user.
7750 SR	BSR	Support per-service and per-content type differentiation of QoS levels and supports distribution of multicast traffic.
7450 ESS	BSA	Aggregate traffic from DSLAMs and other FTTx access devices that are connected to end-user residential gateways.

DSLAMs or other access nodes are connected to Ethernet access ports on the broadband service aggregator. Typically, a single VLAN for each customer is set up between the access node and the BSA. This a configuration enables the application of consistent per-customer policies, such as QoS, filtering, and accounting, to be applied on the BSA.

Scaling of traffic and services is done by dividing L2 and L3 functions between the BSA and the BSR. The BSA aggregates traffic over Gigabit Ethernet ports and performs per-customer service queueing, scheduling, accounting and filtering, as described later in this chapter. The BSR terminates L2 access and routes over IP/MPLS with support for all protocols, including multicasting. Time of day QoS policies can be applied using 5620 SAM policy management.

Interconnectivity between BSAs and BSRs is provided by VPLS. VPLS instances can be automatically established using hub-and-spoke or ring topologies. Both can be configured and sites added to the VPLS using the 5620 SAM. Regardless of the fiber plant layout, VPLS enables a full mesh between all sites that are receiving and distributing customer traffic in the TPSDA, ensuring efficient transport and protection from node or fiber failures.

VPLS also provides mechanisms for traffic security, including residential split horizon groups in which direct user bridging is prohibited; ARP and broadcast suppression; DHCP-populated MAC and IP address filtering to prevent denial or service and theft of service using DHCP snooping, and RADIUS or TACACS+ authentication.

Service differentiation and QoS

This TPSDA approach provides a model based on call admission for video and VoIP, with the need to guarantee delay, jitter, and loss characteristics after the service connection is accepted. The architecture also meets the different QoS needs of HSI, namely per-user bandwidth controls, including shaping and policing functions that have little or no value for video and VoIP service delivery.

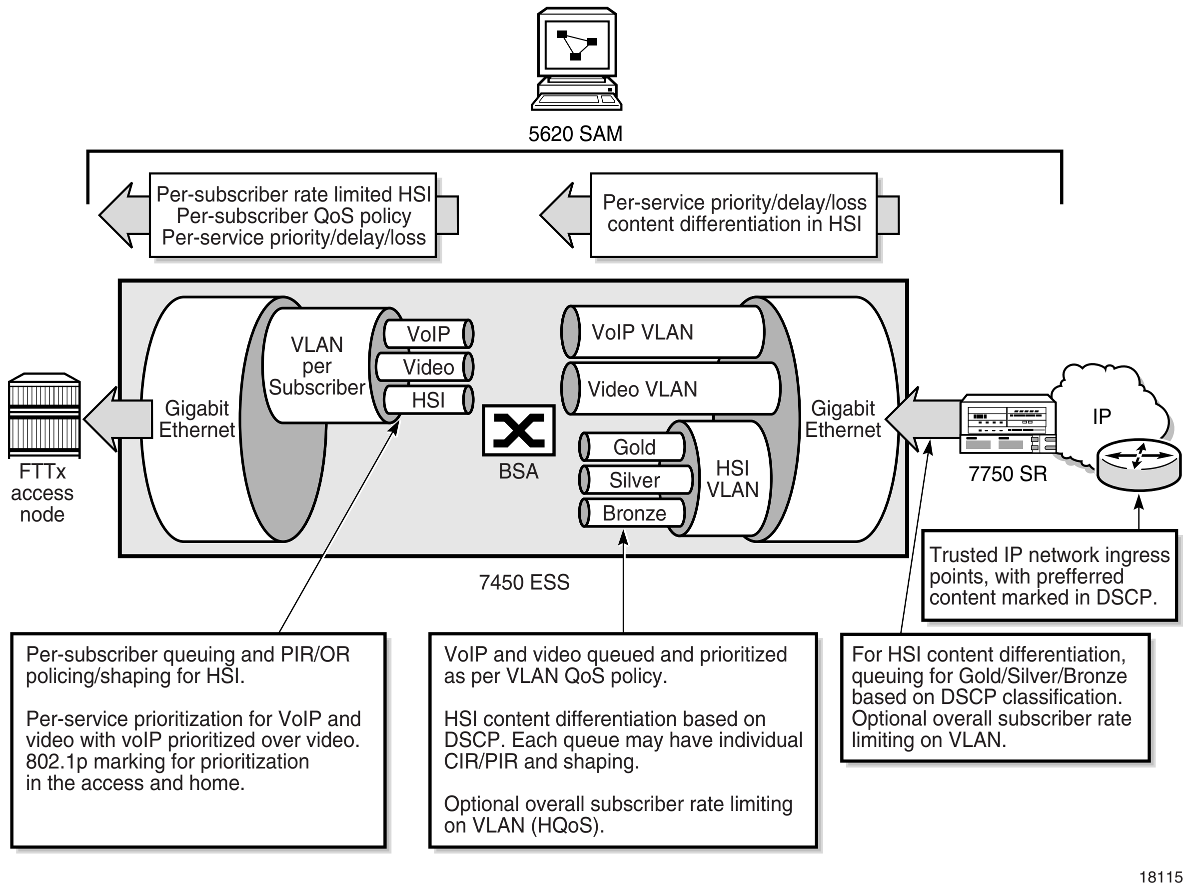
In conjunction with the architecture's support for content differentiation, this approach enables differentiated service pricing within high-priority data packages, also known as HSI. The distribution of QoS policy and enforcement across BSA and BSR allows the service provider to implement meaningful per-user service level controls. Sophisticated and granular QoS in the BSA allows the service provider to deliver truly differentiated IP services differentiation based on the user as well as on the content.

In the BSR to BSA downstream direction, IP services rely on IP layer classification of traffic from the network to queue traffic appropriately towards the BSA. Under extreme loading (only expected to occur under network fault conditions), lower priority data services and/or HSI traffic are compromised to protect video and voice traffic. Classification of HSI traffic based on source network address or IEEE 802.1p marking allows the QoS information to be propagated to upstream or downstream devices.

The BSR performs service distribution routing based on guarantees required to deliver the service and associated content, rather than on individual end users. The BSR only needs to classify content based on its forwarding class for a specific BSA to ensure that traffic for each service receives the appropriate treatment towards the BSA.

Figure 64-7 shows the downstream QoS configurations.

Figure 64-7 TPSDA downstream QoS configurations

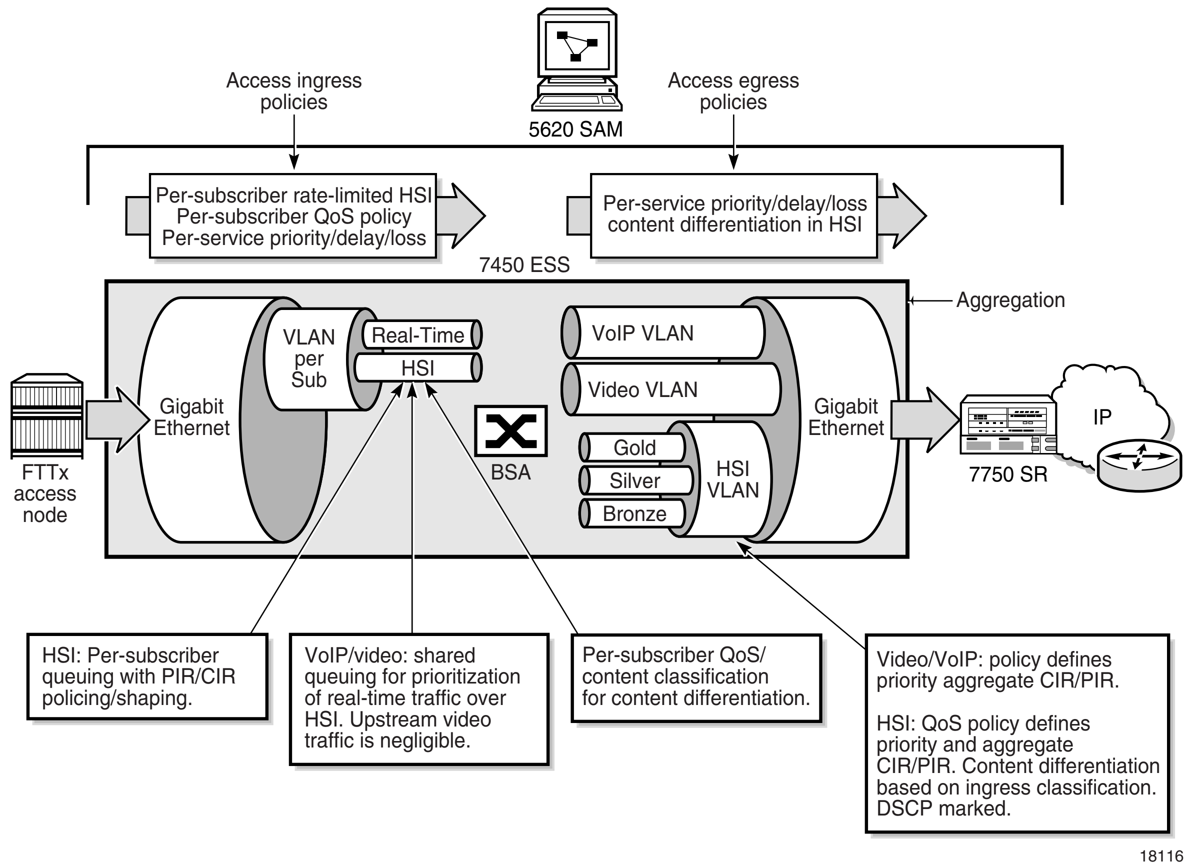


In the BSA-to-BSR upstream direction, traffic levels are substantially lower. Class-based queuing is used on the BSA network interface to ensure that video traffic is forwarded with minimal delay and that preferred data or HSI high-priority data traffic services receive better treatment than for best-effort Internet traffic. The IP edge device (BSR) therefore does not need to enforce per-user policies for hundreds of thousands of users. This function is distributed to the BSAs, and the per-user policies can be implemented on the interfaces directly facing the access nodes.

The BSA is capable of scheduling and queuing functions on a per-service, per-user basis, in addition to performing wire-speed packet classification and filtering based on both L2 and L3 interfaces. In addition to per-service rate limiting for Internet services, service traffic for each user can be rate-limited as an aggregate using a bundled service policy created using the 5620 SAM. These functions allow different users to receive different service levels independently and simultaneously.

Figure 64-8 shows the upstream QoS configurations.

Figure 64-8 TPSDA upstream QoS configurations



When a residential host device, such as a residential gateway or a set-top box in the customer's home, starts up, it requests network information, including the required IP address from a DHCP server. Figure 64-9 shows IP address assignment. See chapter 11 for information about using the 5750 SSC as a DHCP server. See Table 64-4 for more information about DHCP configuration options in the TPSDA.

Figure 64-9 DHCP IP address assignment in the TPSDA

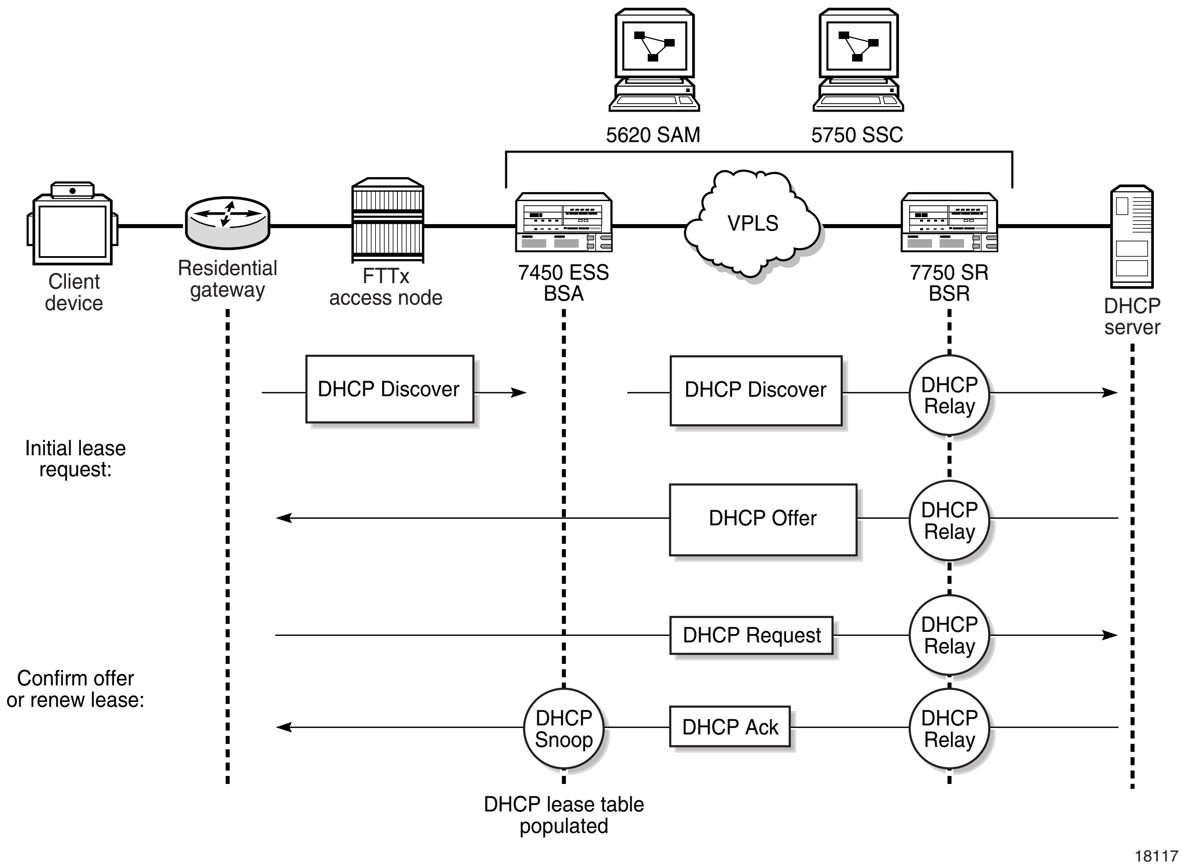


Table 64-4 lists the TPSDA features that you can configure using the 5620 SAM.

Table 64-4 TPSDA features

Feature and use	Notes	Reference
Split horizon groups		
For the TPSDA, there can be no user-to-user communication in the BSA; instead, all communication is done through the BSR. This residential bridging is done using split horizon groups, which ensures that traffic from different SAPs in the same service are not forwarded to other SAPs or spokes.	Traffic arriving on a spoke service tunnel or SAP within the split horizon group is not copied to other SAPs or spoke service tunnels. Traffic is copied to SAPs and spokes in other split horizon groups existing within the same service, such as a VPLS.	See chapter 71 for configuration of split horizon groups.
DHCP		

(1 of 3)

Feature and use	Notes	Reference
For the TPSDA, host devices, such as a residential gateway, SIP phone, or set-top box, use DHCP to obtain IP address and other network configuration information. The client device sends a DHCP discover message to request an IP address. The sequence of events is shown in Figure 64-9.	Information added to the DHCP discover requests may include information added by the FTTx access node or the BSA, for example, the shelf, slot, port, VPI, VCI, or other identifier of the host. You can use the 5620 SAM to configure DHCP relay on the first IP interface in the upstream direction. The BSA or BSR relays the message to a DHCP server. The gateway (residential gateway) IP address indicates to the DHCP server the subnet an IP address should be allocated to for the host.	See the appropriate service configuration chapter, as DHCP, option 82, and DHCP relay are configured at the service level.
DHCP relay DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents intercept the requests and forward them as unicast messages to a DHCP server. DHCP request messages from subscriber hosts are usually sent from the FTTx access node, with information appended to uniquely identify the residential gateway, either by MAC address of the residential gateway or by an option 82 string identifier that indicates the device, port type, rack, shelf, slot, port, and VLAN ID or VPI/VCI of the circuit connected to the residential gateway.	The DHCP relay agent sets the GIADDR in the packet to the IP address of the ingress interface (SAP). You must configure the BSA and BSR devices as DHCP relay agents when the DHCP requests are going to be forwarded to a DHCP server, or a 5750 SSC configured as a DHCP server. The maximum DHCP relay packet size is 1500 bytes.	See the appropriate L3 service (IES and VPRN) or L2 service (VPLS) configuration chapter. See the *5750 SSC Service Manager User Guide* and chapter 11 for more information about configuring the 5750 SSC as a DHCP relay agent.
DHCP lease state table The BSA maintains the identities of hosts that are allowed network access for each SAP on each service.	The lease state information is collected by snooping DHCP acknowledge messages on the SAP, using DHCP snooping. Entries in the DHCP lease state table remain valid for the duration of the IP address lease.	See chapter 20.
DHCP snooping The BSA can copy DHCP packets and inspect them to help secure the system. For example, if malicious user A sends an IP packet requesting a video stream intended for user B, return packets sent to user B could jam B’s connection.	Use the 5620 SAM to configure DHCP snooping for the following purposes: • To insert Option 82 information when the system is not configured for DHCP relay by enabling DHCP snooping on the SAP closest to the host. • To build a DHCP lease state table by enabling DHCP snooping on the service tunnel nearest the network egress and on the SAP closest to the host. • To efficiently associate dynamic hosts with subscriber instances and associated network resources in a triple play service configuration	See the appropriate service chapters for configuration of the lease populate and snooping parameters. See chapter 68 for information about using DHCP snooping for subscriber identification purposes.

(2 of 3)

Feature and use	Notes	Reference
Option 82 The DHCP relay option allows managed devices to append information to the DHCP request that identifies where the DHCP request originated. You can also independently insert Option 82 information when DHCP snooping is enabled on a VPLS SAP. The Option 82 information can be: • The DHCP Option 82 string circuit ID value associated with the 7330 ISAM FTTN, or other ISAM family of nodes in the form ssc(*SSL-7330-1 atm 1/1/04/06:8.35*). The *device port_type rack/shelf/slot/port: VPI:VCI* identifier on the 7330 ISAM FTTN indicates that this is the connection configured for residential use, which is connected to the user's residential gateway. • The DHCP Option 82 string remote ID value associated with the 7330 ISAM FTTN, or other ISAM family of nodes in the form ssc(*remote ID*).	Using Option 82, you can identify: • the circuit ID (service tunnel binding) that is unique to the device relaying the circuit • the remote ID (MAC address) of the host at the far end of the circuit • the subscriber to which a host belongs for the purpose of assigning network resources The maximum DHCP relay packet size is 1500 bytes. If adding Option 82 information to the packet causes the packet to exceed 1500 bytes, the DHCP relay request is forwarded without including the Option 82 information.	See the appropriate service configuration chapter. For DHCP option 82 information inserted because of 5750 SSC DHCP server authentication, see chapter 11. For DHCP option 82 information inserted to identify subscribers, see chapter 68.

(3 of 3)

BTV multicast

This section describes how the 5620 SAM can be used to configure and manage the delivery of BTV multicast traffic streams. See section 64.3 for examples.

Optimizing for broadcast TV means implementing multicast packet replication throughout the network. Multicasting improves the efficiency of the network by reducing the bandwidth and fiber needed to deliver broadcast channels to the end user. A multicasting device can receive a single copy of a broadcast channel and replicate it to any downstream devices that require it, thus substantially reducing the required network resources. This efficiency becomes increasingly important closer to the end user.

Multicast routing overview

Multicast routers direct traffic to several receivers without incurring any additional overhead for the source router or the receivers. In contrast, unicast networks can suffer from increased bandwidth requirements as the number of receivers increases.

In multicast routing, receivers query the source router to request a specific data stream. The multicast group is not restricted by physical location, so long as the hosts can be reached through the Internet. Routers in the network must use IGMP to send and receive multicast data streams.

A multicast-enabled device, such as a switch or router, distributes a data stream to multiple receivers. Multicast packets are replicated in the network by routers that are enabled with PIM, which results in the efficient delivery of data to multiple receivers using less bandwidth.

1 A switch or router distributes a data stream to multiple receivers, such as multicast-enabled PE switches or routers.

2 The multicast-enabled switch or router replicates the data stream, when required, and transmits a copy to each downstream switch or router in the multicast tree.

3 Each client receives the data stream it has subscribed to from the downstream switch or router.

The NEs involved in delivering BTV multicast streams are first preconfigured through CLI for discovery and management by 5620 SAM. After discovery, routing protocols are applied to the NEs using 5620 SAM. Routing, QoS, and network queue policies are then created. On some devices, multicast package and ACL filter policies are created. These policies are applied to NEs during service creation through 5620 SAM.

Content delivery

BTV source traffic consists of one IP multicast stream per broadcast channel. As a multicast stream enters the core network, it is directed by PIM to the RP, which replicates the multicast traffic to all DRs that have requested the specific multicast stream. DRs distribute the multicast stream directly to set-top receivers or through an M-VPLS to BTV VLAN rings to which customer set-top receivers are connected. Multicast streams are forwarded only to those set-top receivers that have requested them through IGMP and are entitled to them as subscriber hosts.

Content management

Multicast package policies on some devices define the available multicast addresses (BTV channels) for end users in a BTV network. Typically, a root package policy which includes all BTV channels associated with a 5620 SAM customer service is created. Subsets of the root policy are then created as BTV content packages to which end customers can subscribe. ACL filter policies on CE devices ensure that only the channels to which an end customer has subscribed are delivered to the customer set-top receiver.

PIM

PIM uses RPF to correctly forward multicast packets down a distribution tree, using the independent multicast and unicast routing tables created by the 7450 ESS in mixed mode or the 7750 SR. The unicast routing table is populated by the unicast routing protocols, such as OSPF, BGP, IS-IS, or static routes, which can also be configured to submit routes to the multicast routing table.

Depending on the configuration of the PIM routing instance, RPF can use the unicast routing table, the multicast table populated by the unicast routing protocols, or both to determine the upstream sources of multicast streams. PIM forwards a multicast packet only if it is received on an upstream interface that is associated with a source address of an upstream router. This RPF check assures that there are no loops in the distribution tree.

PIM uses a multicast domain to group receiver hosts on a router called the rendezvous point (RP). A bootstrap router (BSR) elects an RP from available candidates. The BSR manages RP information, disseminates it to all PIM routers in the multicast domain, and elects a new RP in the case of RP unavailability.

A receiver host becomes a member of a multicast domain by sending an IGMP join request for a multicast stream to a PIM designated router (DR). If the router does not currently receive the multicast stream, PIM updates the DR routing table with the receiver host IP address and requests the multicast stream from the RP. The RP adds the router to the distribution tree. Packets sent to the multicast IP address are propagated down the distribution tree to the receiver host. DRs use the RP as the source for a multicast stream unless a source with a lower path cost is available.

PIM stops sending a multicast stream to a router when it determines that there are no active receiver hosts for the multicast stream in that branch of the distribution tree.

MVR on VPLS

PIM is not supported on 7450 ESSs. When receiver hosts are connected to a PIM DR by way of a 7450 ESS, MVR must be configured on the switch. MVR allows multicast traffic to be forwarded downstream from the DR to the receiver host over an MVR VPLS.

IGMP

IGMP is a multicast protocol which service providers can use to establish multicast group memberships on a LAN. Within the LAN, end users use IGMP to communicate with a local multicast router, which then uses PIM to distribute the IGMP messages to other local and remote multicast routers. Multicast routers send regular membership queries to IGMP hosts which respond with membership reports. Multicast routers can use these reports to determine which hosts are interested in receiving particular multicast messages.

IGMP operates above the network layer on IPv4 networks.

MLD and MLD-snooping

The Multicast Listener Discovery protocol is essentially the IPv6 version of IGMP. It is used by IPv6 routers to discover the presence of multicast listeners (that is, nodes that wish to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

MLD version 2 (MLDv2) is designed to be interoperable with MLD version 1 (MLDv1). MLDv2 adds the ability for a node to report interest in listening to packets with a specific multicast address only from specific source addresses or from all sources except for specific source addresses.

While 5620 SAM currently does not support MLD, it does support MLD-snooping. The 7x50 and 7710 SR routers allow the enabling of MLD snooping for VPLS services.

64.3 BTV multicast configuration examples

Figure 64-10 shows a simple BTV network and three methods of content delivery, examples A, B, and C. The sequence of specific configuration steps for each example follows general device, network and multicast configuration information common to all examples.

Note — In the examples on the following pages, references to "IGMP-snooping" may generally be read as "IGMP- or MLD-snooping", provided the routers employed in the configurations support the MLD protocol.

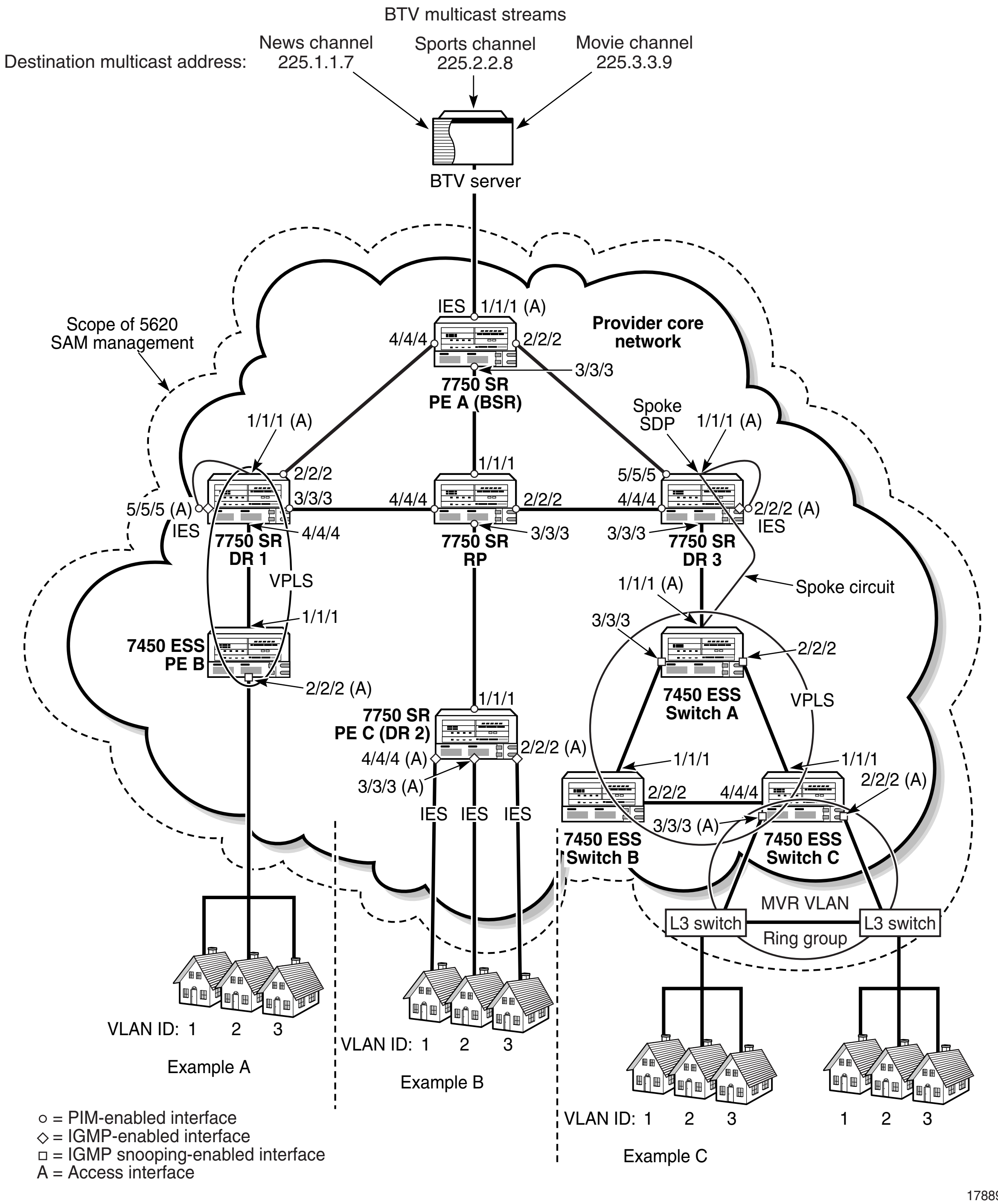
Device preconfiguration

A network device requires CLI preconfiguration before it can be managed by the 5620 SAM. The primary CLI preconfiguration actions for a device are:

- Assigning a system ID to the device
- Enabling and configuring SNMP on the device
- Enabling Telnet access on the device

See chapter 2 and the specific device documentation for more information about enabling device functionality before using the 5620 SAM.

Figure 64-10 BTV multicast delivery examples



After CLI preconfiguration, further actions are required:

- Discover devices, including mediation configuration with CLI user names and passwords.
- Use 5620 SAM to set the discovered device in a managed state.

See chapter 14 for more information about device discovery and management using 5620 SAM.

Network preconfiguration

The core network shown in Figure 64-10 represents a fully meshed group of devices. For simplicity, only the devices relevant to the BTV multicast examples are shown. Network preconfiguration consists of the following sequence of actions:

1. Configure network devices for in-band or out-of-band management. See chapter 13 for more information.
2. Configure a system interface on each device to serve as the identifier for the device. See chapter 30 for more information.
3. Configure network interfaces on each router to establish a full mesh of interconnectivity between devices. In Figure 64-10 the interfaces to be configured are PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; DR 1, port 2/2/2; RP, ports 1/1/1, 2/2/2, and 4/4/4; and DR 3, ports 1/1/1 and 4/4/4. See chapter 30 for more information.
4. Cable the network-interface ports between routers in the core network to establish the physical connectivity shown in Figure 64-10.
5. Use CLI ping commands to check IP connectivity between devices. See the device documentation for more information.
6. Enable IGPs such as RIP, OSPF, or IS-IS on devices according to network size and complexity. See chapter 31 for information about enabling routing protocols.
7. Enable an inter-AS routing protocol such as BGP or OSPF to PE routers, if required. See chapter 31 for more information.
8. Create routing policies as required. Create one multicast group for each BTV multicast destination address during policy creation. See chapter 30 for more information.
9. Configure routing protocols and apply routing policies as required. See chapter 31 for more information.
10. Configure LDP and MPLS, if required. See chapter 31 for information about configuring LDP. See chapter 32 for information about configuring MPLS.
    - Enable MPLS and LDP on the routing instance of each device that is participating in the MPLS network.
    - Assign a Layer 3 interface to the MPLS instance on each MPLS-enabled device.
    - Create a mesh of MPLS paths.
    - Create a mesh of LSPs.
    - Use the 5620 SAM to create MPLS administrative groups, and assign the groups to MPLS interfaces and LSP paths as required.

Multicast configuration common to all examples

The network connections shown between PE A and DR 1 and between PE A and DR 3 represent redundant multicast routes used by PIM in the event of an RP failure. PIM dynamically adjusts to BSR or RP failure by electing a replacement BSR or RP or by using a previously defined backup BSR or RP. PIM chooses the most appropriate source for a multicast stream based on path cost and source availability and bypasses the RP if a better source for a multicast stream is found.

For simplicity, Figure 64-10 does not show routes to PE C (DR 2) from DR 1 or DR 3. As shown, PE C (DR 2) is isolated from multicast traffic in the event of RP failure.

Network multicast configuration common to all three examples involves the following sequence of actions:

1. Enable IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 31-36 for more information.
2. Configure IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 31-37 for more information.
3. Enable PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 31-32 for more information.
4. Configure PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 31-33 for more information.
    - Specify PE A as the candidate bootstrap router.
    - Specify RP as the candidate rendezvous point. You can also specify it as a static RP for a multicast domain, if there are multiple BTV domains, and configure a second router as a redundant RP.
    - Specify IES as the Apply to parameter value on routers PE A, DR 1, PE C (DR 2), and DR 3.
5. Create PIM interfaces at PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; RP, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4; DR 1, ports 2/2/2 and 3/3/3; DR 2, port 1/1/1 and DR 3, ports 4/4/4 and 5/5/5. See Procedure 31-35 for more information.
6. Create QoS, scheduling, and accounting policies for the ingress BTV traffic. See chapter 46 for more information.
7. Create an IES from PE A, port 1/1/1, to the BTV multicast provider's network. See Procedure 73-1 for more information.
    - Enable PIM on the IES SAP during IES creation.

Example A configuration

In Example A, IGMP join requests from residential hosts ingress a VPLS SDP. IGMP snooping on the VPLS registers the join requests on the local switch. The switch sends the requests over the VPLS, which is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream then traverses the VPLS and is sent to end users.

1. Configure PE B, port 1/1/1 and DR 1, port 4/4/4 as network ports. See Procedure 20-1 for more information.
2. Configure PE B, port 2/2/2 and DR 1, port 1/1/1 as access ports. See Procedure 20-1 for more information.

3 Cable DR 1, port 3/3/3, and PE B, port 1/1/1 to establish physical connectivity.

4 Configure DR 1, port 5/5/5 as an access port. See Procedure 20-1 for more information.

5 Create an IES on DR 1, port 5/5/5. See Procedure 73-1 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

6 Connect a cable between ports 1/1/1 and 5/5/5 on DR 1 as a service cross connect.

7 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 46 for information about policy creation.

8 Create a distributed VPLS with endpoints at PE B, port 2/2/2 and DR 1, port 1/1/1. See Procedure 71-1 for more information.

- Enable IGMP snooping on the VPLS SDP at PE B, port 2/2/2.
- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDP at PE B, port 2/2/2.

Example B configuration

In Example B, an IGMP join request ingresses an IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream is then delivered over an IES to an end user.

1 Configure PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 as access ports. See Procedure 20-1 for more information.

2 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during IES creation. See chapter 46 for information about policy creation.

3 Create IES services on PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 that terminate on the CE set-top devices. See Procedure 73-1 for more information.

- Enable IGMP on each IES SAP during IES creation.
- Apply previously defined QoS, scheduling, filter, and accounting policies to each IES, as required.

Example C configuration

In Example C, IGMP join requests from residential hosts pass over an MVR VLAN to an VPLS. IGMP snooping on the VPLS registers the join requests on the local switch, which passes them over the VPLS to a spoke SDP on the DR. The spoke SDP's port is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the VPLS and MVR VLAN to the end users.

1 Create a BTV MVR VLAN of L3 switches, such as 7250 SAS or Telco devices, in a ring group with endpoints on Switch A, ports 2/2/2 and 3/3/3. See section 69.4 and Procedure 69-5 for more information. For redundancy, the MVR VLAN can be configured with endpoints on different switches. A VLL between the two switches acts as an unbreakable connection.

2 Enable and configure IGMP snooping on the bridge instances for the L3 switches included in the MVR VLAN. See section 31.1 for information specific to 7250 SAS Telco devices or see the specific device documentation if the L3 switch a type not managed by the 5620 SAM.

3 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 46 for information about policy creation.

4 Configure the following as network ports:

- Switch A, ports 1/1/1, 2/2/2, and 3/3/3
- Switch B, ports 1/1/1 and 2/2/2
- Switch C, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4

See Procedure 20-1 for more information.

5 Create a distributed VPLS consisting of Switch A, Switch B, and Switch C. See Procedure 71-1 for more information.

- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDPs.
- Enable and configure IGMP snooping on the VPLS SDPs that are part of the MVR VLAN.
- Ensure that the encapsulation value of the VPLS SDPs that are part of the MVR VLAN matches the MVR VLAN ID.
- Create a split horizon group during VPLS creation to allow later addition of a spoke circuit to the VPLS.
- Configure STP on the VPLS, as required.

6 Configure DR 3, port 2/2/2 as an access port. See Procedure 20-1 for more information.

7 Create an IES on DR 3, port 2/2/2. See Procedure 73-1 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

8 Connect a cable between ports 1/1/1 and 2/2/2 on DR 3 as a service cross connect.

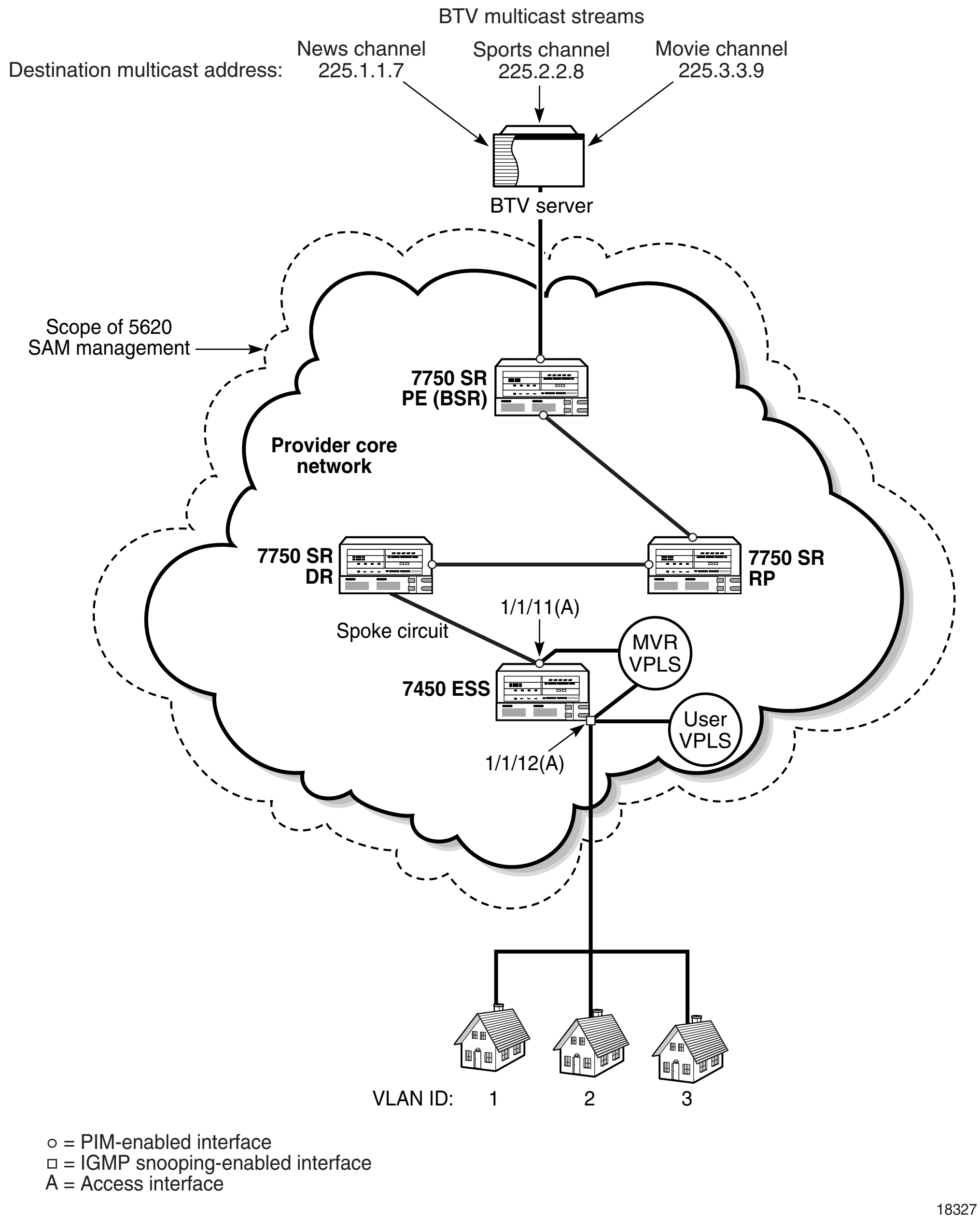
9 Create a VPLS spoke SDP at DR 3, port 1/1/1. See Procedure 71-9 for more information.

Example D configuration

Figure 64-11 shows an example of BTV multicast delivery using MVR on VPLS.

See Figure 64-10, and sections “Network preconfiguration” and “Multicast configuration common to all examples” for common network configuration information.

Figure 64-11 BTV multicast delivery using MVR on VPLS example



In Example D, IGMP join requests from residential hosts are sent to a user VPLS on the 7450 ESS. IGMP snooping on the user VPLS registers the join requests on the switch, which sends them to the 7750 SR DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the MVR VPLS to the user VPLS, from which the multicast stream is sent to the end users.

1 Create a multicast package policy to apply to the 7450 ESS that belongs to the MVR VPLS. See chapter 49 for more information.

2 Configure the following ports as access ports. See Procedure 20-1 for more information.

- 7450 ESS, port 1/1/11
- 7450 ESS, port 1/1/12

3 Create an MVR VPLS on the 7450 ESS with SAPs 1/1/11 and 1/1/12. Apply the previously defined multicast package policy to the MVR VPLS.

4 Create a user VPLS on SAP 1/1/12 of the 7450 ESS.

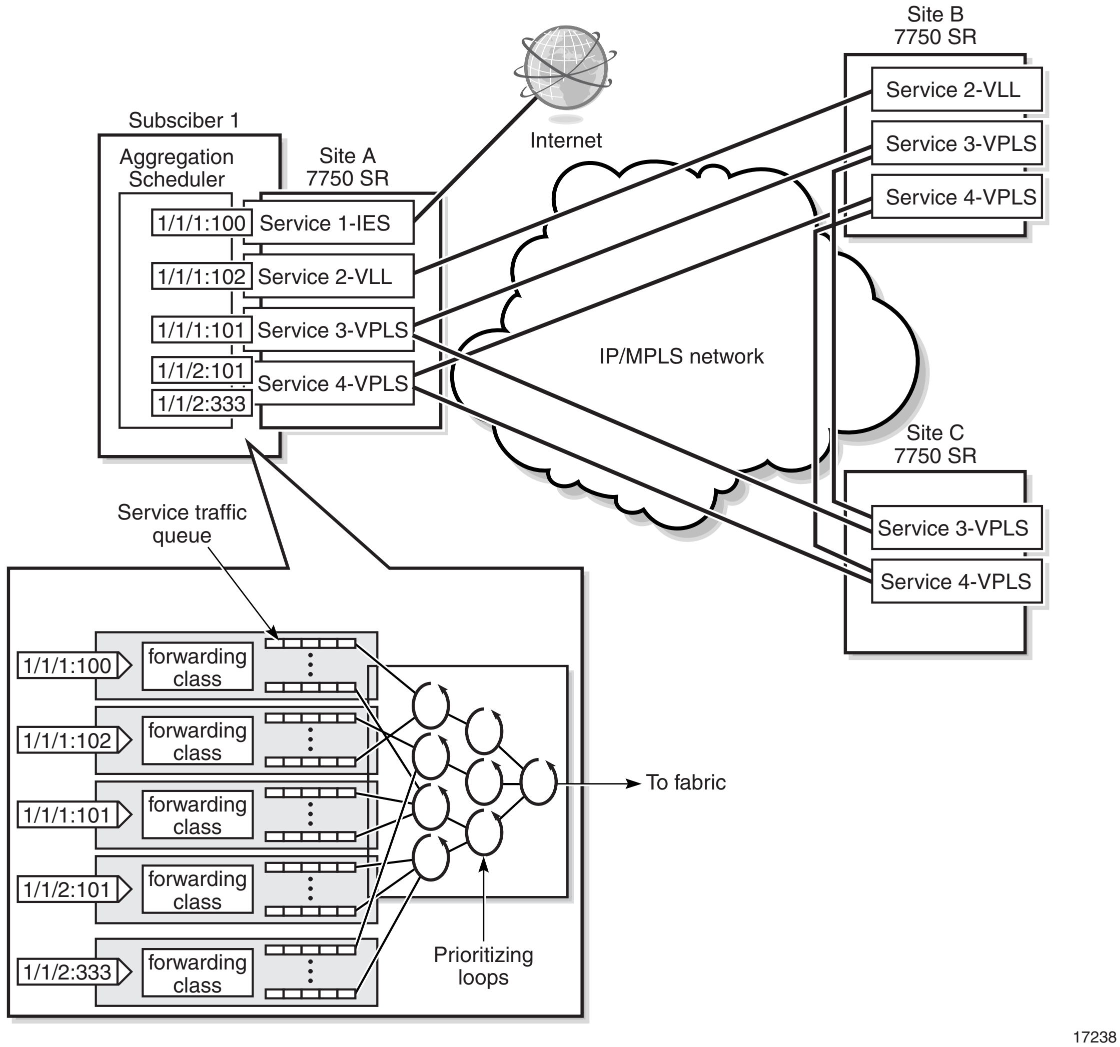
- Associate the user VPLS with the previously created MVR VPLS to identify the MVR VPLS as the source of the multicast traffic.
- Enable and configure IGMP snooping on the site.

5 Create a spoke circuit between the 7450 ESS (endpoint 1/1/11) and the 7750 SR DR.

64.4 Sample network configuration using QoS

Figure 64-12 shows an example of a service configuration using QoS.

Figure 64-12 Example of a service configuration using QoS



In this configuration, the following services are provisioned:

- Service 1: IES for Internet access, which requires a CIR of 10 Mb/s and a PIR of 100 Mb/s
- Service 2: VLL service for FTP connectivity between Site A and Site B, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s
- Service 3: VPLS for video-conference service over sites A, B, and C, which requires a CIR of 20 Mb/s and a PIR of 50 Mb/s
- Service 4: VPLS for voice traffic, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s

The cumulative rate at site A needs to be limited to 70 Mb/s.

The following high-level steps are required to create the Figure 64-12 configuration with rate limiting using QoS at Site A. Similar steps are required to configure QoS for Subscriber 1 on Sites B and C:

1 Configure a scheduler policy.
2 Create Subscriber 1.
3 Create the aggregation scheduler for Subscriber 1 on site A and assign ingress and egress scheduler policies to the aggregation scheduler.
4 Create IES, VLL, and VPLS for Subscriber 1.
    - Specify sites for the services.
    - Specify access interfaces for the sites.
    - Specify the aggregation scheduler policy for the access interfaces.
    - Bind the services to tunnels for transport through the IP/MPLS network.

Access interfaces 1/1/1:100, 1/1/1:101, 1/1/1:102, and 1/1/2:101 participate in the aggregation scheduler and are usually rate limited by the rate specified in the scheduler policy.

Access interface 1/1/2:333 does not participate in scheduler policy; rate limiting is specified by the queue values.

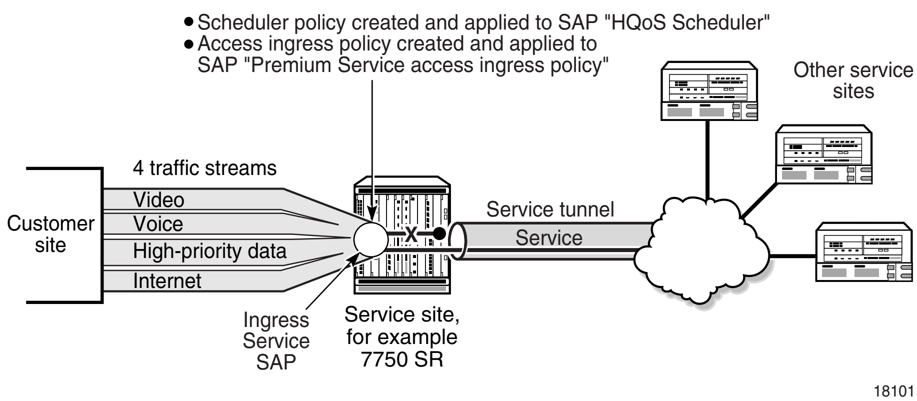
If one of the access interfaces does not participate in the scheduler aggregator, it may be managed by a separate scheduler policy.

64.5 Sample SAP QoS configuration

You can use 5620 SAM to configure and enforce traffic rate limiting, based on the priority of the traffic entering the ingress SAP of a service. This configuration limits bandwidth, to ensure that SLAs are met and higher priority traffic is processed first.

Figure 64-13 shows traffic of different priorities from a customer site to an ingress SAP.

Figure 64-13 Example showing ingress traffic to a service SAP



Based on the example, use the 5620 SAM client GUI to perform the following actions:

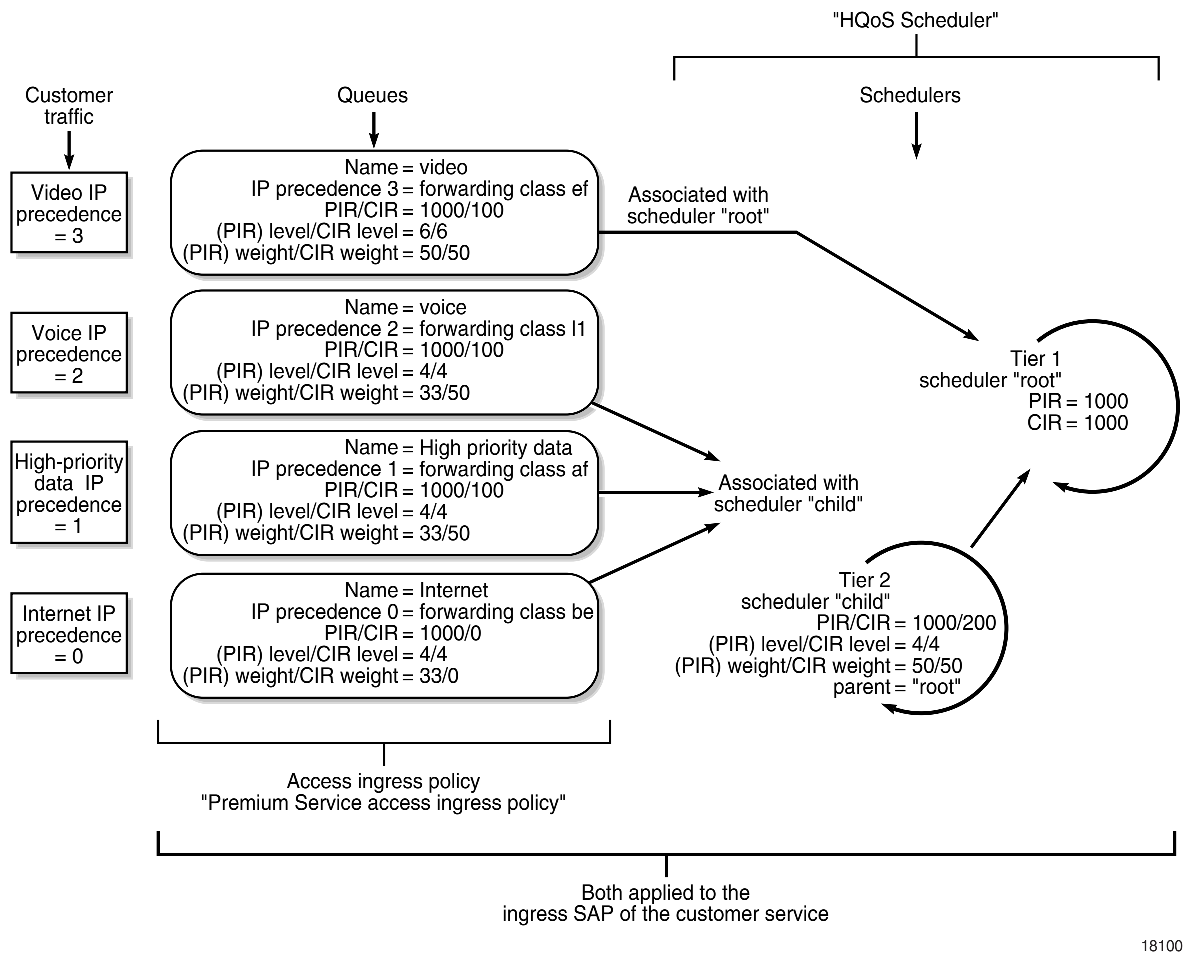
- Configure a parent scheduler that handles scheduling for a child scheduler.

  Note — You do not have to configure a parent tier 1 scheduler for a child tier 2 scheduler. You can create a tier 2 scheduler on its own, with no parent. This example is meant to show hierarchical QoS.

  - Add a root tier 1 scheduler
  - Add one child tier 2 scheduler with the root scheduler as a parent
- Create an access ingress policy named Premium service access ingress policy.
  - Create 4 queues within the access ingress policy, one for each type of traffic from the customer site.
  - Associate each queue with a forwarding class
  - Classify the incoming customer site traffic to a forwarding class. For this sample, IP precedence is used to classify traffic. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.
  - Associate each queue with the appropriate scheduler.
- Apply the schedulers and access ingress policy to the appropriate L2 or L3 interface for the customer service, for example, a VPLS L2 interface.

Figure 64-14 shows how traffic is handled based on the ingress access policy and scheduler queue handling applied to the ingress service SAP.

Figure 64-14 Traffic handling based on ingress access policy and scheduler queue



In this sample:

- higher-priority video traffic, with IP precedence bit 3 set, goes into queue 4 with a PIR of 1000 Kb/s and a CIR of 100 Kb/s. This traffic is handled by the tier 1 scheduler. The levels and weights associated with the video queue (forwarding class of ef, level of 6, PIR/CIR weights of 50/50) ensure this traffic gets all required bandwidth.
- all other traffic goes into its appropriate queues, based on the mapping of the IP precedence bit with the forwarding class.
- The voice, high-priority data, and Internet queues are serviced by the tier 2 scheduler.
- Because the voice and high-priority data queues have higher PIR/CIR weight than the Internet queue, when there is contention for bandwidth, the voice and high-priority data queues are processed first.

Preconfiguration

1 Before you begin, you must have:

- the service ingress SAP configured as access
- all necessary cabling and network routing protocol configurations complete to handle routing packets to and from the CPE equipment

Configuration

2 Choose Policies→QoS→SROS QoS→Scheduler→Scheduler from the 5620 SAM main menu. The manage scheduler policies form opens.

3 Click on the Create button. The scheduler policy create form opens.

4 Configure the parameters. Set the displayed name to High QoS.

5 Click on the Schedulers tab button.

6 Click on the Create button. The scheduler entry form opens.

7 Create a root, tier 1 scheduler entry,

i Configure the parameters.

- Displayed name to root
- tier to 1
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 1000

ii Click on the OK button. The root scheduler appears in the list of scheduler entries.

8 Create a child, tier 2 scheduler entry.

i Click on the Create button.

ii Configure the parameters.

- Displayed name to child
- tier to 2
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 200
- Parent scheduler to root, using the Select button to choose root from the list.
- Level (PIR level) to 4
- Weight (PIR weight) to 50
- CIR Level to 4
- CIR Weight to 50

iii Click on the OK button. The child scheduler appears in the list of scheduler entries.

9 Click on the Apply button.

10 Close the Scheduler form.

11 Choose Policies→QoS→SROS QoS→Access Ingress from the 5620 SAM main menu. The manage access ingress policies form opens.

12 Click on the Create button. The access ingress policy create form opens.

13 Configure the parameters. Set the displayed name to Premium service access ingress policy.

14 Click on the Queues tab button. Create four queues. For this sample, default queue 1 is modified, and three new queues are added. The default multicast queue 11 is unchanged.

15 Select queue 1 from the list.

i Click on the Properties button. The queue 1 edit form opens.

ii Configure the parameters.

- Displayed Name to Internet
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 0

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 0
- Pir (kbps) to 1000

v Click on the OK button.

16 Add queue 2.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 2
- Displayed Name to High-priority traffic
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

17 Add queue 3.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 3
- Displayed Name to Voice
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

18 Add queue 4.

i Click on the Create button. The queue create form opens.

ii Configure the parameters.

- ID to 4
- Displayed Name to Video
- Scheduler to root by using the Select button and choosing root from the list
- Level (PIR level) to 6
- CIR Level to 6
- Weight (PIR weight) to 50
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- Rate Type to kbps
- Policed to false
- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

19 Click on the Apply button to save the changes. Confirm the action.

20 Associate each queue with a forwarding class.

i Click on the Forwarding Classes tab button.

ii Click on the Create button. The forwarding class create form opens.

iii Configure the parameters.

- Forwarding class to be
- Queue ID to 1. This is the best-effort Internet traffic queue.

iv Click on the OK button. Confirm the action.

v Click on the Create button. The forwarding class create form opens.

vi Configure the parameters.

- Forwarding class to af
- Queue ID to 2. This is the high-priority data traffic queue.

vii Click on the OK button. Confirm the action.

viii Click on the Create button. The forwarding class create form opens.

ix Configure the parameters.

- Forwarding class to l1
- Queue ID to 3. This is the voice traffic queue.

x Click on the OK button. Confirm the action.

xi Click on the Create button. The forwarding class create form opens.

xii Configure the parameters.

- Forwarding class to ef
- Queue ID to 4. This is the highest priority, video traffic queue.

xiii Click on the OK button. Confirm the action.

21 Click on the Apply button. Confirm the action.

22 Associate the IP precedence bits of the incoming customer traffic with the forwarding class. The forwarding class is already associated with a queue. For this sample, IP precedence bits are used to associate different types of traffic with the forwarding class. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.

i Click on the Precedence tab button.

ii Click on the Create button. The precedence create form opens.

iii Configure the parameters to associate IP precedence 0 (Internet traffic from the customer site) with forwarding class be (the be forwarding class is associated with queue 1)

- Precedence is 0
- Forwarding Class is be

iv Click on the OK button. Confirm the action. The association between precedence 0 and the be forwarding class is added to the list.

v Click on the Create button. The precedence create form opens.

vi Configure the parameters to associate IP precedence 1 (high-priority data traffic from the customer site) with forwarding class af (the af forwarding class is associated with queue 2)

- Precedence is 1
- Forwarding Class is af

vii Click on the OK button. Confirm the action. The association between precedence 1 and the af forwarding class is added to the list.

viii Click on the Create button. The precedence create form opens.

ix Configure the parameters to associate IP precedence 2 (voice traffic from the customer site) with forwarding class l1 (the l1 forwarding class is associated with queue 2):

- Precedence is 2
- Forwarding Class is l1

x Click on the OK button. Confirm the action. The association between precedence 2 and the l1 forwarding class is added to the list.

xi Click on the Create button. The precedence create form opens.

xii Configure the parameters to associate IP precedence 3 (video traffic from the customer site) with forwarding class ef (the ef forwarding class is associated with queue 3)

- Precedence is 3
- Forwarding Class is ef

xiii Click on the OK button. Confirm the action. The association between precedence 3 and the ef forwarding class is added to the list.

23 Click on the Apply button. Confirm the action.

24 Click on the Relations tab button to view the associations between the IP precedence bit number, the forwarding class, and the queues.

25 Associate a service SAP with the created High QoS scheduler and the created Premium service access ingress policy. There are many ways to associate policies with L2 or L3 interfaces used as service SAPs, for example, from the service creation form or the port properties form. This sample modifies an existing L2 interface for an existing VPLS.

- **i** Choose Manage→Service→Services from the 5620 SAM main menu. The manage services form opens.
- **ii** Set the filters and click on the Search button. A list of filtered services appears.
- **iii** Select the service and click on the Properties button. The service form opens.
- **iv** Click on the L2 Access Interfaces tab button.
- **v** Choose an interface and click on the Properties button. The L2 interface edit form opens.
- **vi** Click on the QoS tab button.
- **vii** Configure the parameter. Use the Select button to set the Ingress Policy to Premium service access ingress policy. The policy ID and displayed name appear.
- **viii** Click on the Schedulers tab button.
- **ix** Configure the parameter. Use the Select button to set the Ingress Scheduler to High QoS. The displayed name appears.
- **x** Click on the Apply button to save the changes. Confirm the action.

64.6 Workflow to implement QoS on an OmniSwitch

1 Enable QoS on the OmniSwitch and configure global settings such as global port parameters, default disposition for flows, and timeouts. The parameters that you need to configure globally depend on the types of policies that you need to configure.

Typically, you do not need to change any of the global defaults. See step 36 of Procedure 31-54 for information.

2 Configure QoS port parameters, which includes setting QoS parameters on a per port basis. Typically you do not need to change the port defaults. See step 19 of Procedure 20-34 for information.

3 Configure QoS policies. See chapter 47 for more information.

64.7 Workflow to implement QoS on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR

Planning and configuration

1 Perform network planning activities:

   i Determine the required types of services or applications; for example, voice, video, and data.

   ii Review SLAs.

   iii Perform traffic engineering activities at the IP/MPLS core level to ensure that resources are available.

2 Configure the IP and MAC ACL filters, as required. Refer to Procedures 48-1 and 48-3 for more information.

3 Configure the slope policies. Refer to Procedures 47-8 and 47-10 for more information.

4 Configure the scheduler policies. Scheduler policies can be shared between ingress and egress policies, depending on your specific requirements. Refer to Procedure 47-15 for more information.

5 Configure the port scheduler policies. Refer to Procedure 47-18 for more information.

6 As required, create the aggregation schedulers. Refer to Procedure 47-29 for more information.

7 Configure the access ingress policies. Refer to Procedure 47-1 for more information.

   i Configure the forwarding classes.

   ii Configure the queues.

   iii Map QoS markings on ingress packets to the forwarding classes.

   iv Map forwarding classes to the queue definitions.

   v Map queue definitions to the scheduler policies.

8 Configure the access egress policies. Refer to Procedure 47-3 for more information.

   i Configure the queues.

   ii Map forwarding classes to the queue definitions.

   iii Map queue definitions to the schedulers policies.

9 Configure the network policies. Refer to Procedure 47-6 for more information.

i Configure for ingress:

- Map QoS markings on ingress packets to the forwarding classes.
- Map forwarding classes to the queue definitions.

ii Configure for egress:

- As required, configure remarking.
- As required, map QoS markings to the forwarding classes.

10 Configure the network queue policies. Refer to Procedure 47-12 for more information.

11 Configure the time of day policies.

i Configure the time ranges. Refer to Procedure 50-1 for more information.

ii Create time of day suites. Refer to Procedure 50-2 for more information.

Application of policies and schedulers to equipment and interfaces

12 Associate the slope policies with ports or daughter cards. Refer to Procedures 20-1 and 19-24 for more information.

13 Associate the network queue policies with MDAs. Refer to Procedures 20-1 and 20-46 for more information.

Configuration of customers and services

14 Configure the customers. Refer to the appropriate service chapter for more information.

15 Create the customer services, and assign policies during the configuration. Refer to the appropriate service chapter for more information.

16 Assign the aggregation schedulers at the interface level, if required. Refer to the appropriate service chapter for more information.

64.8 5620 SAM QoS policies

Policies group and manage the various QoS elements used to determine how traffic is routed.

- access ingress policies
  Specify how QoS marking is interpreted, how customer traffic is mapped into queues, and how queues are classified.
- access egress policies
  Specify how customer traffic is mapped into queues, specify queue classification, queue parameters, and QoS marking.
- network policies
  Specify QoS marking to forwarding class mapping on ingress and QoS marking to forwarding class mapping on egress.

- network queue policies
  Specify CIR, PIR, and burst sizes for each queue. Forwarding class to queue mapping is not configurable.
- scheduler policies
  Specify custom settings and a hierarchical structure of virtual schedulers to replace the default hardware schedulers on the device.
- port scheduler policies
  Specify bandwidth allocation at the egress port level.
- HSMDA scheduler policies
  Specify schedulers to define egress port and ingress scheduler behavior on an HSMDA.
- slope policies
  Specify WRED settings to customize how in-profile and out-of-profile traffic is processed in hardware buffers, applied to daughter cards or ports.
- HSMDA slope policies
  Specify settings for controlling how the depth of HSMDA queues is managed.
- ATM QoS policies
  Specify ATM QoS settings to customize ATM traffic parameters including service category and shaping.

Figure 64-15 shows where QoS policies are applied at the service level.

Figure 64-15 Service-level view of policies

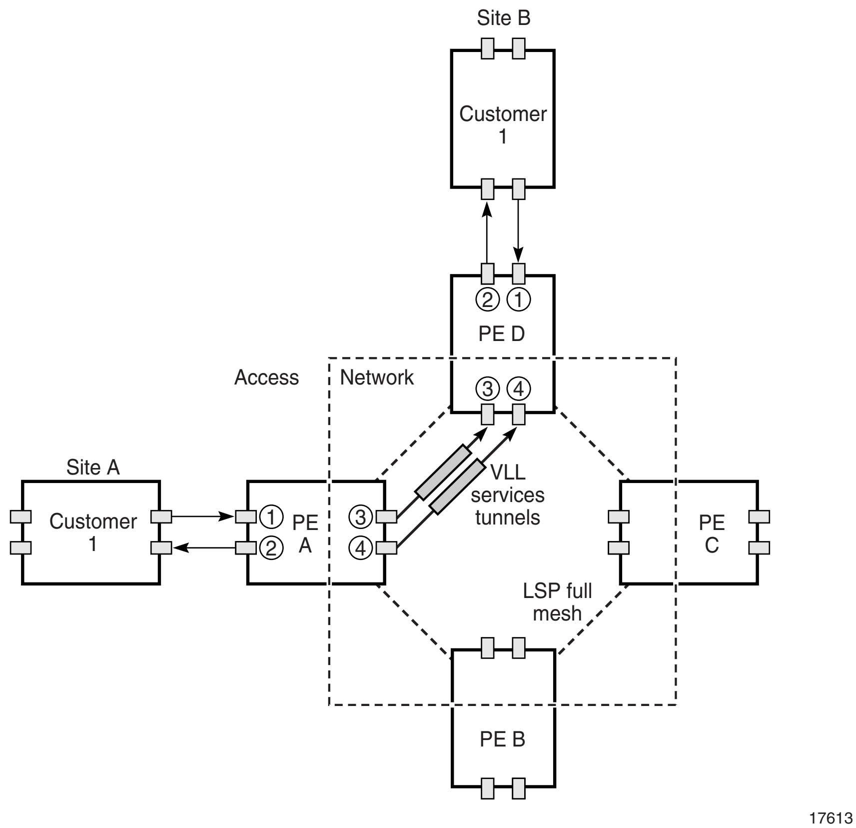
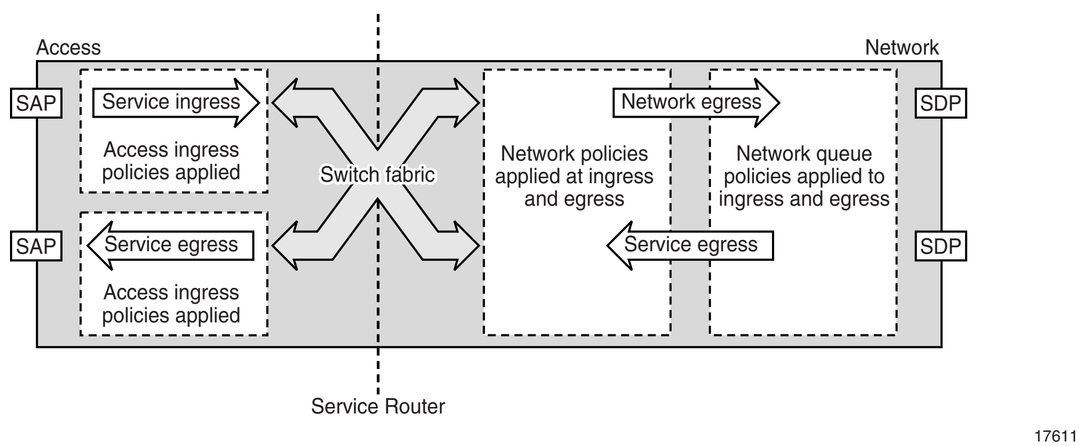


Figure 64-16 shows where policies are applied on a device with respect to access and network ingress and egress traffic.

Figure 64-16 Types of traffic on a device and applied policies



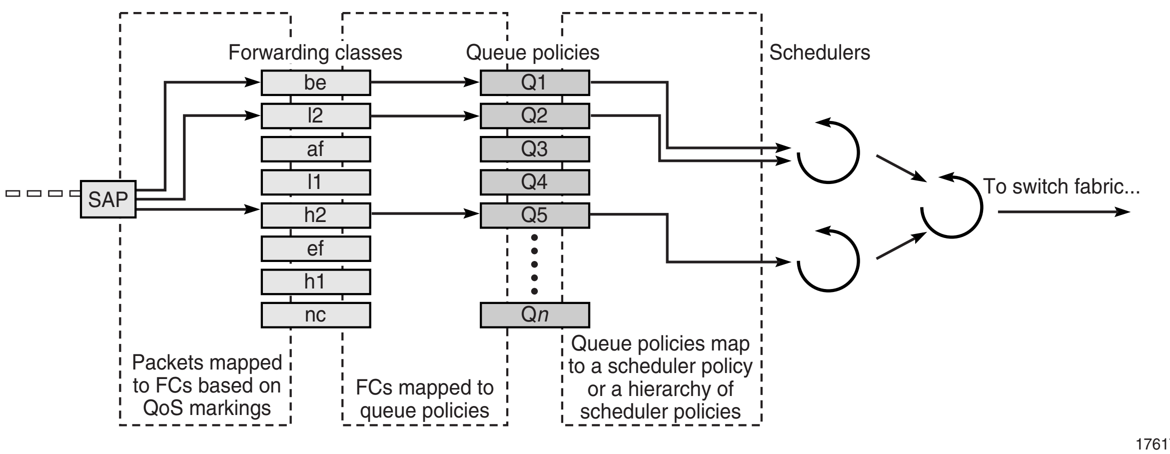
Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS characteristics on ingress. Participation in access ingress policies is defined when access interfaces are configured or modified. Access ingress policies include:

- mapping of QoS marking, such as dot1p, DSCP, and precedence, and IP/MAC address information to forwarding classes
- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 64-17 shows the access ingress policy elements.

Figure 64-17 Access ingress policy elements



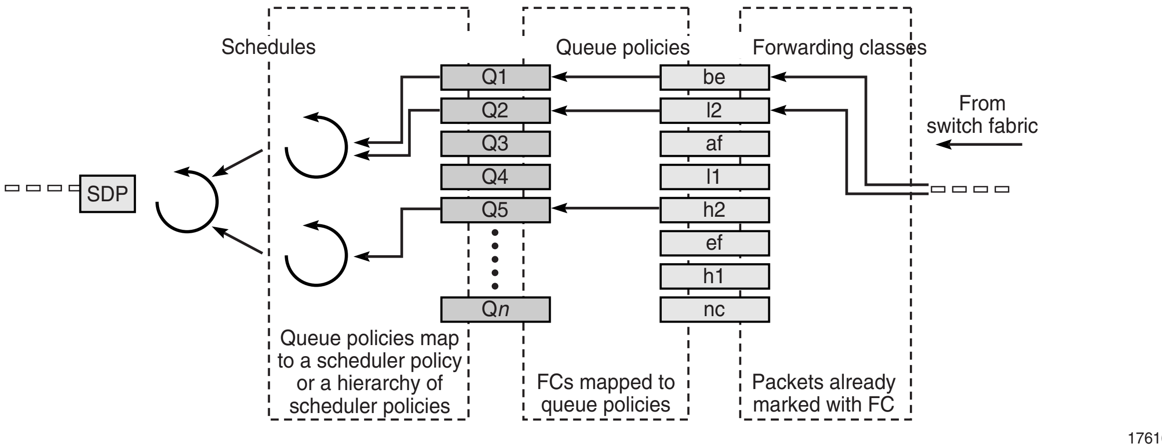
See "Access ingress policies" in section 47.1 for more information about access ingress policies.

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS characteristics on egress. Participation in Access egress policies is defined when access interfaces are configured or modified. Access egress policies include:

- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 64-18 Access egress policy elements



In Figure 64-18, packets are marked with an FC, either by:

- ingress policy if the packet was received on the same device
- in the tunnel transport encapsulation if received using a service tunnel

See "Access egress policies" in section 47.1 for more information.

Network policies

Network policies define egress QoS markings and ingress QoS interpretation for traffic on core network IP interfaces. A network policy defines:

- DSCP name mapping to forwarding classes
- LSP EXP value mappings to forwarding classes
- whether QoS remarking is enabled

Figure 64-19 shows the sequence of how the elements of network and network queue policies are applied at ingress.

Figure 64-19 Network and network queue policy elements on ingress

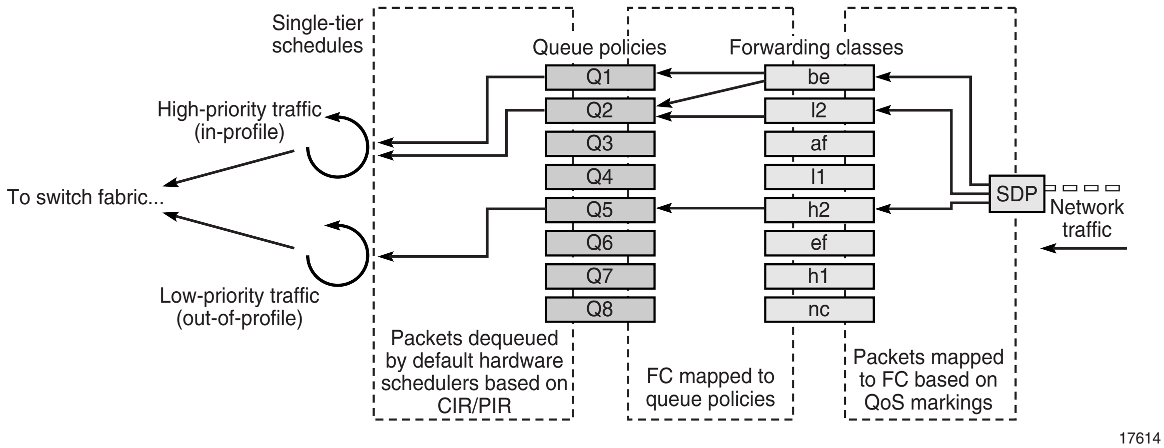
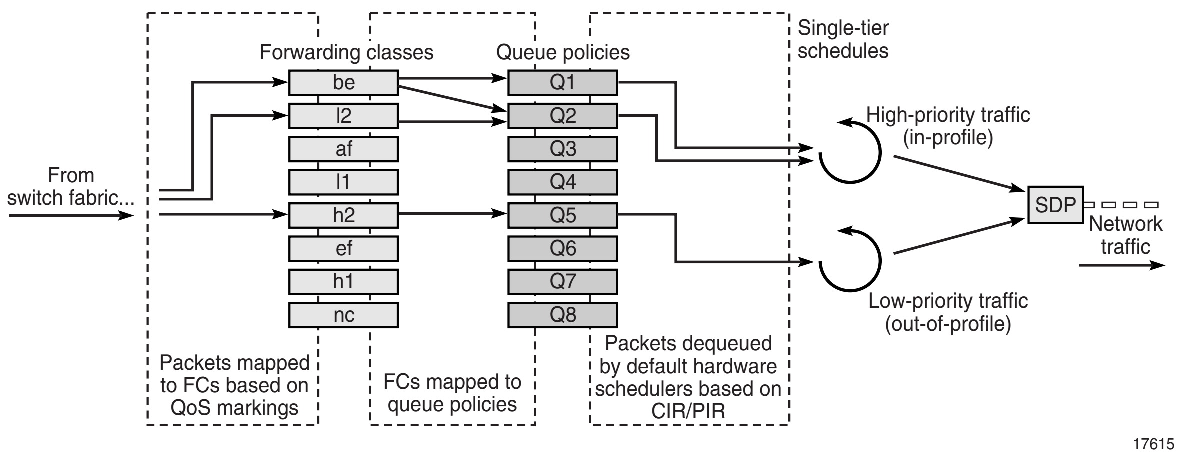


Figure 64-20 shows the sequence of how the elements of network and network queue policies are applied at egress.

Figure 64-20 Network and network queue policy elements on egress



See “Network policies” in section 47.1 for more information.

Network queue policies

Network queue policies define the network forwarding class queue characteristics for core egress network ports and for ingress on MDAs.

See Figure 64-19 and Figure 64-20 for the sequence of how the different elements of network and network queue policies are applied on ingress in and on egress.

The queued packets are serviced by single-tier schedulers on the device and are forwarded to a single destination switch fabric port or a network interface.

See “Network queue policies” in section 47.1 for more information about network queue policies.

Scheduling

Scheduling defines the order and method for how packets which are enqueued in different queues, are dequeued. Ingress schedulers control the data transfer between the queues and the switch fabric. Egress schedulers control the data transfer between the egress queues and the switch fabric. Packets are not actually forwarded to schedulers, but are forwarded from the queues directly to ingress and egress interfaces. Participation in scheduler policies is defined when access interfaces are configured or modified. There are two types of scheduling:

- Single-tier scheduling is the hardware-based default method for scheduling queues on the device. There are no configurable parameters for single-tier schedulers. When a scheduler policy is not specified for an access interface, rate limiting is specified by the values specified in the queue and scheduling is performed by the default hardware scheduler on the device. Single-tier scheduling consists of a pair of scheduling priority loops in the 7750 SR and bases scheduling on the CIR and the PIR set in the queue policy. One loop is for scheduling high-priority (in-profile) traffic, and the other loop is for low-priority (out-of-profile) traffic.
- Virtual hierarchical (multi-tier) scheduling can provide more flexible scheduling for access ingress and egress interfaces, and determine how queues are scheduled. They are defined using a Scheduler policy, and can be configured to override default hardware scheduling. You can create up to three tiers of virtual schedulers.

  Aggregation schedulers are used to share a scheduler policy across a number of ports or daughter cards. This can be useful when a number of ports or cards are dedicated to the same customer. See “Scheduler policies” in section 47.1 for more information about configuring aggregation schedulers.

Port scheduler policies

Port scheduler policies define the bandwidth allocation based on the available bandwidth at the egress port level. A port scheduler policy manages a bandwidth allocation algorithm that represents a virtual multi-tier scheduling hierarchy.

The port scheduler allocates bandwidth to each service or subscriber that is associated with an egress port. Egress queues on the service may have a child association with a scheduler policy on the SAP or multi-service site. All queues must compete for bandwidth from an egress port. There are two methods of bandwidth allocation on the egress access port:

- **direct association of port scheduler on a SAP or multi-service site with service or subscriber queue**

  A service or subscriber queue is associated with a scheduler on the L2 access interface or multi-service site, and the service-level scheduler policy is associated with a port level scheduler.
- **direct association of port scheduler with service or subscriber queue**

  A service or subscriber queue is associated with a port scheduler. The port scheduler hierarchy allocates bandwidth at each priority level to each service or subscriber queue.

See “Port scheduler policies” in section 47.1 for more information about configuring port scheduler policies.

HSMDA scheduler policies

The port-based scheduler manages forwarding for each egress port on the HSDMA. Each port-based scheduler maintains up to eight forwarding levels. Eight scheduling classes contain each of the queues that are assigned to the port scheduler. Membership in a scheduler is defined by the queue identifier.

The port-based scheduler supports a port-based shaper that is used to create a sub-rate condition on the port. Each scheduling level can be configured with a shaping rate to limit the amount of bandwidth allowed for that level.

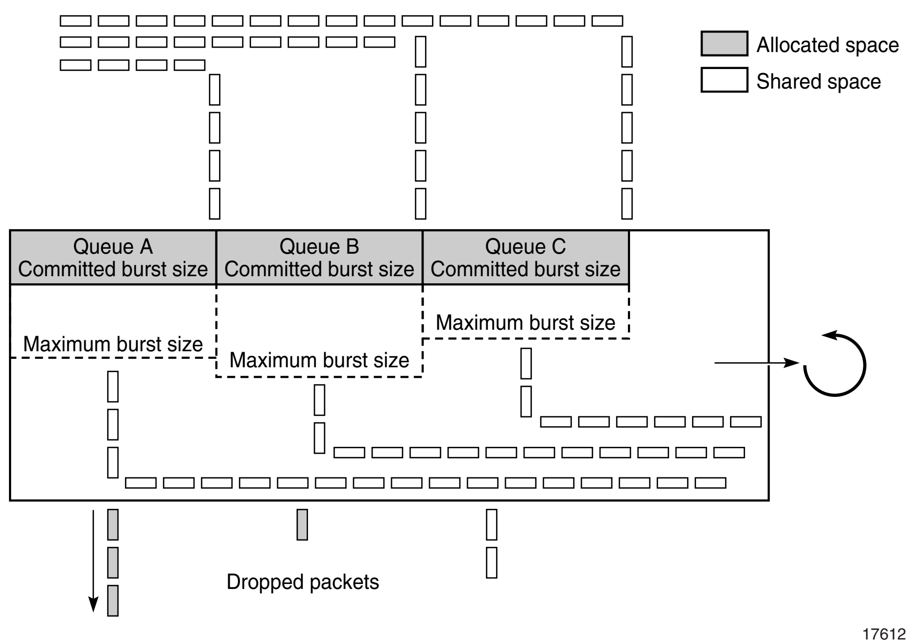
The port-based scheduler allows two weighted groups (group 1 and group 2) to be created. Each group can be populated with three consecutive scheduling classes.

See "HSMDA scheduler policies" in section 47.1 for more information about configuring slope policies.

Slope policies

Slope policies manage how shared buffers are utilized on the SR. When traffic is queued, the WRED slope parameters in the slope policy determine how the traffic is buffered for dequeuing, as shown in Figure 64-21.

Figure 64-21 Slope policy characteristics



All queues are in contention for shared buffer space when they exceed their CBS, and can use their MBS, when space is available in the shared buffer space. The WRED parameters determine whether a packet is discarded or not, and, as a result, determine whether the packet is dequeued. When the shared buffer space exceeds or approaches the maximum percentage defined by the WRED configuration, packets are discarded.

By using two independent slope policy configurations, one for in-profile traffic and one for out-of-profile traffic, you can configure in-profile traffic to receive preferential treatment over out-of-profile traffic.

See “Slope policies” in section 47.1 for more information about configuring slope policies.

HSMDA slope policies

HSMDA slope policies control the HSMDA queues. Each queue supports an index for an HSMDA slope policy table. Each policy in the table consists of two RED slopes (one high priority and another for low priority) to manage queue congestion. HSMDA RED slopes operate on the instantaneous depth of the queue.

A packet that attempts to enter a queue triggers a check to see whether the packet is allowed based on queue congestion conditions. The packet contains a congestion-priority flag that indicates whether the HSMDA is to use the high or low slope. The slope policy containing the slope is derived from the policy index in the queue configuration parameters on the HSMDA.

The RED slope discards are based on the current queue depth before a packet is allowed into the queue. Therefore, a queue may consume buffers that are greater than the configured MBS value based on the size of the packet. After the packet maximum is reached, packets that are associated with the queue are discarded. When the schedule removes packets from the queue, the queue depth decreases, which eventually lowers the depth of the threshold.

See “HSMDA slope policies” in section 47.1 for more information about configuring HSMDA slope policies.

65 — Queue groups

65.1 Queue group overview

Queue groups are objects created on access or network Ethernet port that allow SAP or IP interface forwarding classes to be redirected from standard queue mapping to a shared queue. Access ingress ports support a single queue group for each ingress port. Access egress and network egress ports support the creation of multiple queue groups.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

See "Queue Group Template policies" in section 47.1 for more information.

Port queue groups

The port queue group contains the queue groups that are created based on the queue IDs defined within the associated Ingress/Egress Queue Group Template policies. Port queue groups are supported on Ethernet ports and can be created on ports within a LAG. Port queue groups are not supported on HSMDA Ethernet ports and VSM MDAs. Network egress queue groups are not supported on the following IOM-1 cards:

- IOM-10 G
- IOM-20 G
- IOM-20 G-B

You can create a port queue group after creating an Ingress/Egress Queue Group Template policy.

Note — You must use the same name for the port queue group and Ingress/Egress Queue Group Template policy.

LAGs

When a port queue group is created on a LAG, the group is individually instantiated on each link in the LAG. The queue parameters for a queue within the queue group are used for each port queue.

You can create, modify, or delete a port access ingress, access egress, or network egress queue group on the primary port of the LAG. (The primary port is the port with the lowest port ID.) The NE automatically replicates the create, modify, or delete action for the queue group on all other ports within the LAG.

Note — The 5620 SAM does not allow you to create, modify, or delete an Access Ingress, Access Egress, or Network Egress queue groups on non-primary ports.

When you add a port to a LAG, the port must use the same access ingress, access egress, or network egress queue groups as the existing ports on the LAG. To ensure this requirement for the port, the 5620 SAM implements the following sequential comparison:

- number of queue groups
- queue group names
- number of queue overrides
- individual parameters

Note — Alcatel-Lucent recommends that you add all required ports to the LAGs before the configuration of the port queue group.

Access SAP forwarding class-based redirection

Typically, each SAP has dedicated ingress and egress queues that are only used by that specific SAP. Individual SAP queuing requires a more complex provisioning model to configure the ingress and egress SLAs of the SAP. The configuration requires service awareness at the aggregation locations in the network. There are cases where individual SAP queuing is not preferred. In these cases, you can use a shared queue or an individual port queue model. You can configure a shared queue by creating access ingress and access egress queue groups, and mapping the forwarding classes of the SAP to the queues within the queue group.

You can configure forwarding class redirection on a SAP to a queue group queue ID using the access ingress/egress QoS policy. In each policy, the forwarding class to queue ID mapping can specify a queue group name.

See section 65.2 for more information.

Network IP interface forwarding class-based redirection

You can create queue groups on egress network ports to provide network IP interface queue redirection. A single set of egress port-based forwarding class queues are available by default, and all IP interfaces on the port share the queues. The creation of a network queue group allows one or more IP interfaces to selectively redirect forwarding classes to the group to override the default behavior.

The redirection of the egress forwarding class on an IP interface to an egress queue group queue ID is provisioned using the Network policy. The actual queue group name can be specified when the Network Policy is applied to the IP interfaces.

You can configure dedicated queues for each IP interface using network egress queue groups.

See section 65.3 for more information.

Queue group statistics

The packets sent to the queue of a SAP are statistically tracked by a set of counters associated with the queue group queue, not the SAP counters. The tracking occurs when a forwarding class is redirected to an ingress or egress port queue group queue.

On a network interface, the counter sets are created for each egress IP interface, not for each egress queue. The same counter set is used when a forwarding class for an egress IP interface is redirected from the default egress port queue to a queue group queue.

See the *5620 SAM Statistics Management Guide* for information about managing statistics collection and to view a list of the MIB counters that are available for collection using the 5620 SAM.

Configuration validation rules

Table 65-1 describes the validation rules that are enforced for NE queue group configurations.

Table 65-1 Validation requirements for queue group configurations

Component		Validation action
Ingress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
	Policy deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the policy.
Egress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
		The deletion is blocked if there is a Network policy with a forwarding class that is associated with the queue ID.
	Policy deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the policy.
		The deletion is blocked if there is a network IP interface associated with the policy.
Port queue groups	Port Access Ingress Queue Group deletion	The deletion is blocked if there is an Access Ingress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Port Access Egress Queue Group	The deletion is blocked if there is an Access Egress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Network Egress Queue Group	The deletion is blocked if there is a network IP interface that is directly or indirectly bound to the port by a LAG associated with the port queue group.

(1 of 2)

Component		Validation action
Access SAP forwarding class-based redirection	Access Ingress QoS policy	The Queue Group name must exist as an Ingress Queue Group Templates policy.
		The Queue ID must exist within the associated Ingress Queue Group Templates policy with appropriate queue type.
		Only one unique Queue Group may be referenced within one Access Ingress QoS policy.
		The current Access Ingress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Ingress Queue Group does not exist.
		The current Access Ingress QoS policy should not be applied to a SLA Profile policy.
	Access Egress QoS policy	The Queue Group name must exist as an Egress Queue Group Templates policy.
		The Queue ID must exist within the associated Egress Queue Group Templates policy.
		The current Access Egress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Egress Queue Group does not exist.
		The current Access Egress QoS policy should not be applied to a SLA Profile policy.
	Access Ingress/Egress QoS policy assignment	When an Access Ingress/Egress QoS policy with a forwarding class redirection to a Queue Group Queue ID is applied to a SAP, the following configurations are verified: • The Queue Group specified in any forwarding class redirection must exist as an Access Ingress/Egress Queue Group on the port associated with the SAP • The Access Ingress/Egress QoS policy with Queue Group specified cannot be applied to SLA Profile policy
Network IP Interface forwarding class-based redirection	Network policy	The specified queue ID must exist within the Egress Queue Group Templates policy for all IP interfaces where the Network policy is applied. If the Network policy is currently applied to any IP interfaces without an explicit Network Egress Queue Group specified, the configuration fails.
		The following configurations are verified when the Network policy is applied to a network IP interface: • The network policy with a redirected queue group cannot be applied to the network IP interface without a port binding. • The redirected queue group name must exist as a Network Egress Queue Group on the port or LAG associated with the IP interface. • The queue ID for the redirected queue group in the associated Network policy must exist within the associated Egress Queue Group Templates policy.

(2 of 2)

65.2 Workflow to configure access SAP forwarding class-based redirection

The following workflow describes the steps required to configure access SAP forwarding class-based redirection.

1 Create a global ingress/egress queue group template policy.

   a Create an ingress queue group template policy. See Procedure 47-22 for more information.

   b Create an egress queue group template policy. See Procedure 47-23 for more information.

2 Distribute the global ingress/egress queue group template policy to the NEs. See Procedure 46-1 for more information.

3 Create an ingress/egress queue group on the Ethernet access port. See Procedure 20-1 for more information.

4 Create or configure a global access ingress/egress QoS policy with the forwarding class mapped to the queue group queue ID. The queue group queue ID must be included in the queue group template policy. Perform the following, as required:

   a Create an access ingress QoS policy. See Procedure 47-1 for more information.

   b Create an access egress QoS policy. See Procedure 47-3 for more information.

5 Distribute the global access ingress/egress QoS policy to the NEs. See Procedure 46-1 for more information.

6 On the SAP configuration form, assign the access ingress/egress QoS policy to the SAP bound to the port on which the access ingress/egress queue group was created in step 3. Perform one of the following, as required:

   a Assign an access ingress/egress QoS policy to an L2 access interface on a VLL. See Procedure 70-13 for more information.

   b Assign an access ingress/egress QoS policy to an L2 access interface on a VPLS. See Procedures 71-3, 71-13, and 71-14 for more information.

   c Assign an access ingress/egress QoS policy to an L2 access interface on an IES. See Procedure 73-8 for more information.

   d Assign an access ingress/egress QoS policy to an L2 access interface on a VPRN. See Procedure 74-13 for more information.

   e Assign an access ingress/egress QoS policy to an L3 access interface on an IES. See Procedure 73-1 for more information.

   f Assign an access ingress/egress QoS policy to an L3 access interface on a VPRN. See Procedure 74-2 for more information.

65.3 Workflow to configure network IP interface forwarding class-based redirection

The following workflow describes the steps required to configure a network IP interface forwarding class-based redirection.

1. Create a new global egress queue group template policy. See Procedure 47-23 for more information.

2. Distribute the global egress queue group template policy to the NEs. See Procedure 46-1 for more information.

3. Create an egress queue group on the Ethernet network port. See Procedure 20-1 for more information.

4. Create or configure a global network policy with the forwarding class mapped to the queue group queue ID. The queue group queue ID must be included in the egress queue group template policy, which is specified when the network policy is applied to the IP interface. See Procedure 47-6 for more information.

5. Distribute the global network policy to the NEs. See Procedure 46-1 for more information.

6. On the network interface configuration form, assign the network policy and the queue group template policy to the network interface. The network egress queue group must be created on the port to which the network interface is bound. The network egress queue group must use the same name as the selected queue group template policy. See Procedure 30-7 for more information.

65.4 Workflow to configure statistics collection for queue groups

The following workflow describes the steps required to enable the collection of queue groups statistics.

1. Create or modify an accounting policy. See Procedure 4-2 for more information on creating an accounting policy.

2. Configure the Type parameter on the Accounting Policy form to collect one of the following statistics options:

   - Combined Queue Group
   - Queue Group Octets
   - Queue Group Packets

   See Procedure 4-2 for more information on specifying the type and frequency of accounting statistics collection.

3. Enable the Collect Accounting Statistics parameter on the port's queue group Physical Port (Edit) form. See Procedure 20-1 for more information on adding an access ingress/egress queue group on an Ethernet access port.

66 — Virtual ports

66.1 Virtual port overview

A 7750 can act as a Broadband Network Gateway (BNG), fairly distributing bandwidth among the subscriber host sessions by accounting for the packet encapsulation overhead and ATM bandwidth expansion for each type of broadband session. In this way, subscriber packets are less likely to be dropped downstream in the DSLAM DSL port. Furthermore, the BNG shapes the aggregate rate of each subscriber and the aggregate rate of all subscribers destined to a given DSLAM to prevent congestion of the DSLAM.

In the BNG application, when a set of per FC queues are applied to each subscriber host context, the host per FC queue packet rate is overridden by the rate provided in the Radius access-accept message. This rate represents the ATM rate that will be seen on the last mile and includes the encapsulation offset and the per packet expansion due to ATM segmentation into cells at the BSAN.

In order to enforce the aggregate rate of each destination BSAN, a virtual port must be configured. Virtual ports are scheduling nodes that operate like port schedulers, with the exception that multiple virtual ports can be created on the egress context of an acess/hybrid Ethernet port. A virtual port and a port scheduler cannot exist simulatenously on a single port.

Virtual ports can be created on a port that is a member of a LAG. When a virtual port is created, modified, or deleted on the primary port of a LAG, this action is replicated on all other ports within the LAG. These actions can only be perfoemd on the primary port. When a port is added to a LAG, it must have the same virtual ports defined as the existing ports on the LAG. The name of a virtual port is local to the port on which it is applied, but must be the same for all member ports of a LAG.

Virtual ports are supported on Ethernet ports on IOM3/IMM in 7750, 7750 sparrow, and 7450.

Virtual ports are not supported on SR1 or ESS1 platforms, HSMDA Ethernet ports, or VSM MDA.

Virtual port statistics can be collected and displayed for all queues forwarding to a virtual port configured on an egress of an Ethernet port. This is only supported on an 7750 SR or 7740 SR equipped with a 2 x XP MDA IOM-3. The collected data is available on the Statistics tab of the Egress Scheduling Virtual Port properties form.

SLA Profiles

A subscriber host queue with the port-parent option enabled can be scheduled within the context of a port scheduler policy associated with a port or a virtual port. To specify that a subscriber host queue with the port-parent option enabled be scheduled within the context of a virtual port, the Scheduler Type parameter must be set to Virtual port when configuring an SLA Profile.

See Procedure 68-13 for more information.

Subcriber Profiles

The subscriber aggregate rate is adjusted to account for the fixed offset and per packet variable expansion of the last mile for the specific session used by the subscriber host. The adjustment is based on the average frame size.

See Procedure 68-14 for more information.

66.2 Virtual ports procedures

The following procedures describe how to configure and manage virtual ports.

Procedure 66-1 To configure virtual ports

1 Configure an SLA Profile, as described in Procedure 68-13.

2 Configure a Subscriber Profile, as described in Procedure 68-14.

3 Perform one of the following:

   a Create a virtual port using the navigation tree, as described in Procedure 66-2.

   b Create a virtual port using the Port QoS form, as decribed in Procedure 66-3.

Procedure 66-2 To create virtual ports using the navigation tree

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to create virtual ports and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Shelf icon.

4 Expand to the port level and click on an access/hybrid Ethernet port. The Port form opens with the General tab displayed.

5 Click on the Egress Scheduling Virtual Port tab button.

6 Click on the Create button. The Egress Scheduling Virtual Port (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Aggregate Rate Limit (kbps)

8 Click on the Select button in the Port Scheduler Policy panel to choose a Port Scheduler Policy. The Select Port Scheduler Policy form opens.

Note — You cannot select a port scheduler policy for the virtual port if you've already selected a port scheduler policy for the associated channel. Likewise, selecting a port scheduler policy for the virtual port will prevent you from selecting a port scheduler policy for the associated channel.

9 Select a Port Scheduler Policy and click on the OK button. The Select Port Scheduler Policy form closes and the Egress Scheduling Virtual Port (Create) form reappears with the Port Scheduler Policy information displayed.

10 Click on the Host Matching tab button.

11 Click on the Create button. The Host Matching form opens.

12 Configure the Destination String parameter.

13 Click on the OK button. A confirmation dialog box appears.

14 Click on the OK button. The Egress Scheduling Virtual Port (Create) form reappears with the Destination String information displayed.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The Port form reappears with the Egress Scheduling Virtual Port information displayed.

17 Click on the OK button. A confirmation dialog box appears.

18 Click on the Yes button. The Port form closes.

Procedure 66-3 To create virtual ports using the Port QoS form

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Manage Port QoS list form opens.

2 Select Egress Scheduling Virtual Port from the object type drop-down list.

3 Click on the Create button and choose Virtual Port(s). The Egress Scheduling Virtual Port (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description

5 Click on the Select button in the Port Scheduler Policy panel to choose a Port Scheduler Policy. The Select Port Scheduler Policy form opens.

6 Select a Port Scheduler Policy and click on the OK button. The Select Port Scheduler Policy form closes and the Egress Scheduling Virtual Port (Create) form reappears with the Port Scheduler Policy information displayed.

7 Click on the Host Matching tab button.

8 Click on the Create button. The Host Matching form opens.

9 Configure the Destination String parameter.

10 Click on the OK button. A confirmation dialog box appears. Click on OK.

11 Click on the Targeted Physical Ports tab button.

12 Click on the Add button. The Select Site form opens.

13 Click on the Search button. The form displays a list of sites.

Note — The count displayed on the form reflects the total number of found ports and may not align with the number of applicable ports displayed in the list.

14 Select a site in the list and click on the OK button. The Select Site form closes and the Egress Sheduling Virtual Port (Create) form reappears with the site information displayed.

15 Click on the OK button. The Egress Scheduling Virtual Port (Create) form closes and the Port QoS list form reappears.

16 Close the form.

Procedure 66-4 To copy virtual ports

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Port QoS list form opens.

2 Select Egress Scheduling Virtual Port from the object type drop-down list.

3 Click on the Search button. The form displays a list of virtual ports.

4 Select a virtual port in the list and click on the Copy... button. The Egress Scheduling Virtual Port (create) form opens with the virtual port's values populated.

5 Click on the Targeted Physical Ports tab button.

6 Click on the Add... button. The Select Site form opens.

7 Click on the Search button. The form displays a list of sites.

8 Select one or more sites in the list and click on the OK button. The Select Site form closes and the Egress Sheduling Virtual Port (create) form reappears with the site information displayed.

9 Click on the OK button. The Egress Scheduling Virtual Port (create) form closes and the Port QoS list form reappears.

10 Close the form.

67 — Customer configuration and service management

67.1 Customer configuration and service management overview

The 5620 SAM allows you to create and manage customers and the services they subscribe to.

An end user is the recipient of application content that is delivered through a service. The service is a means of transport for the application content and is owned by a service customer. For example, an end user subscribes to a high-speed Internet access service, and the Internet access service is owned by a service provider who is a service customer of the network provider. The 5620 SAM provides only customer management, not end-user management. Customers were called subscribers in earlier versions of 5620 SAM.

On the General tab of a customer management form, you can configure basic customer information. From the other tabs on the form, you can configure and monitor 5670 RAM thresholds, services, service sites, templates, and aggregation schedulers for a customer.

Each customer is associated with an ID that is assigned when the customer account is created. When configuring a service, you can use the ID or the listed name of the customer to associate a customer with a service.

A customer can own more than one service, but an individual service is owned by only one customer. Two or more services can be joined to form a composite service. The individual services that comprise the composite service can be owned by different customers. Customers that own services participating in a composite service are associated with the composite service.

Managing the size of a service associated with a customer

A customer service can become very large over time if new sites are continually added. As a result, a service containing thousands of sites or instances may become cumbersome to manage. The 5620 SAM allows you to easily move sites from one service to another in order to reduce the overall size of a particular service.

Sites can be moved for the following service types supported in 5620 SAM: VPRN, VPLS, MVPLS, IES, and all VLL types. However, the following restrictions apply:

- You can only move a site between like services, that is, from one VPLS to another VPLS, but not between a VPLS and a VPRN, for instance.
- The services that you are moving sites to and from must have the same Service ID.
- The services that you are moving sites to and from must have the same Customer ID.

If you need to reduce the size of an existing service, you can use another existing service that meets these restrictions. Alternatively, you can create a new service of the same type for this purpose. The Service ID and Customer ID of the new service must match those of the existing service.

In addition, if the existing service which you are moving sites from is a member of a composite service, then the newly-created service you are moving the sites to will also belong to the same composite service. This action will only take place after moving the sites that form the composite service connectors.

67.2 Workflow to create and manage customers and the services they subscribe to

1 Create customers that will purchase and use services. See Procedure 67-1.

- Configure or modify key customer contact and billing information.
- Assign or associate equipment or resources to customers, as appropriate.

2 As required, configure the system preferences of the services that are associated with customers. See Procedure 67-2.

3 Create, modify, or delete existing services (such as IES, VPLS, VPRN, or VLL) that are associated with customers. See the relevant service chapter in this guide.

4 Monitor or troubleshoot customers, based on SLAs between the customer and the service provider.

- Retrieve customer information and contact the customer when service problems or maintenance windows occur. See Procedure 67-3.
- View a service map for a customer. See Procedure 67-4.
- Perform diagnostics as appropriate to troubleshoot service problems associated with customers. See the relevant service chapter in this guide.
- As required, view and modify the inventory of all the services, interfaces, circuits, and other information that are associated with a customer. See Procedure 67-5.
- If required, reduce the service size associated with a customer by moving sites from one service to another. See Procedure 67-6.

5 As required, delete a customer from the 5620 SAM database. See Procedure 67-7.

67.3 Customer configuration and service management procedures

The following procedures describe how to configure and manage customers and the various aspects of their services. Detailed procedures on specific service type creation and modification are provided in the relevant service chapters.

Procedure 67-1 To create a customer

1 Choose Manage→Service→Customers from the 5620 SAM main menu.

2 Click on the Create button. The Customer (Create) form opens with the General tab displayed. The General tab shows contact and billing information.

3 Configure the parameters.

- Auto-Assign ID
- ID
- Name
- Description
- Address
- Phone Number
- Contact
- Email

The information in the General tab is used to create a database of customer information, including contact information, so that the customer can be contacted if there is a service or equipment problem.

4 As appropriate, configure any other tabs on the Customer (Create) form. See step 5 in Procedure 67-5.

5 Click on the Apply button to save the customer information.

Procedure 67-2 To configure the system preferences of services associated with a customer

Perform this procedure to configure the system preferences for customer services.

Caution — Changing a System Preference parameter value may affect one or more existing 5620 SAM services. Do not change a parameter value from the default without contacting Alcatel-Lucent technical support.

Note — The System Preferences parameters are configurable only by a user with administration privileges.

1 Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens with the Services tab displayed.

2 Configure the parameters:

- Auto Discover Composite Services
- Maximum number of sites that can be moved
- Default Service Priority
- Suppress VPRN SNMP Community String Warning
- Remove Empty Service
- Multi-Segment Tunnel Selection
- CAC (Native Ethernet PBB)
- Alarm Aggregation to Composite Service
- Whenever a site is added to a service in SAM, propagate the Service Name to Site Name

3 Click on the OK button. The System Preferences form closes.

Procedure 67-3 To list the services associated with a customer

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with Service (Service Management) selected in the filter list.
2. Use the filter for the Customer Name column to filter the list results.
3. Click on the Search button. A list of services matching the filter criterion appears.

Procedure 67-4 To view a service map for a customer

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Choose Service (Service Management) from the object drop-down list.
3. Use the filter for the Customer Name column to filter the list results.
4. Click on the Search button. A list of services matching the filter criterion appears.
5. Choose a service from the list and click on the Topology View button. A dialog box appears.
6. Click on the Yes button. The Service Topology - *Service Name* form opens.
7. Scroll the map to view the topology of the service and the devices used for the service.
8. Click on the Close button to close the map.

Procedure 67-5 To modify and manage customer information

Use this procedure to view and modify the inventory of all the services, interfaces, circuits, and other information that are associated with a customer.

1. Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.
2. Click on the Search button to search for the customer whose information you want to change. The search results are displayed in the bottom panel of the form.
3. Choose the customer and click on the Properties button. The Customer (Edit) form opens.
4. View or modify the information for the customer.

Each tab lists parameters you can view or modify, or functions that you can perform, related to customer management.

- The General tab lists the ID, the customer name, and contact information.
- The 5670 RAM Parameters lists the Apdex and MOS thresholds that can be set by the customer. See step 5b for more information.
- The Services tab lists which services such as VPLS, VPRN, or VLL are associated with the customer.
- The Sites tab lists the PE devices used by the customer.
- The Aggregation tab lists aggregation schedulers defined for the customer. See chapter 47 for information about creating aggregation schedulers.
- The Associated Templates tab lists service templates used to create services for the customer.
- The Spans tab lists the span of control over customers.

5 Modify customer information as appropriate:

a To modify text in the General tab:

i Make the changes in the appropriate fields and click on the OK button. A dialog box appears.

ii Click on the Yes button. The Customer (Edit) form closes.

b Configure the 5670 RAM parameters as listed below:

- Reporting Name
- Apdex scores below this threshold are unacceptable quality
- Apdex scores below this threshold are poor quality
- Apdex scores below this threshold are fair quality
- Apdex scores below this threshold are good quality
- MOS scores below this threshold are bad quality
- MOS scores below this threshold are poor quality
- MOS scores below this threshold are fair quality
- MOS scores below this threshold are good quality

c To modify site or template information for the customer:

i Click on the appropriate tab button on the Customer (Edit) form.

ii Select the object in the list for which you want to modify information.

iii Click on the Properties button. The configuration form for the object opens.

Caution — Ensure configuration changes do not affect customer services. Use the Turn Down button to turn down a service before making any changes that may affect customer traffic.

iv Modify the information on the configuration form as required and click on the OK button. The changes are saved and the object configuration form closes.

Procedure 67-6 To perform a service size reduction associated with a customer

Perform the following procedure to move sites between services:

1 If you plan to move more than 25 sites at a time then go to step 2. Otherwise, go to step 5.

2 Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens.

3 Configure the Auto Discover Composite Services parameter. The maximum number of sites you can move at a time is 50.

Note — The Auto Discover Composite Services parameter can only be modified by a user with administration privileges.

4 Click OK. The System Preferences form closes.

5 If you are planning to move sites between two existing services then go to step 8. If you need to create a new service to move sites to then go to step 6.

6 Refer to the relevant service creation chapters in this guide to create the new type of service that you need. This new service must exist before you can move sites from an existing service.

When creating the new service, observe the following requirements:

- The new service must be of the same type as the existing service
- The Auto-Assign ID functionality for the Service ID must not be enabled. The Service ID must be manually entered, and it must match the Service ID for the existing service
- The Customer ID of the new service must match that of the existing service
- You do not need to create any sites for the new service

7 Return to step 8 in this procedure once you have created the new service.

8 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

9 Choose Service (Service Management) from the object drop-down list.

10 Click the Search button. A list of available services is displayed.

11 Select the service that you want to move sites from and click the Properties button. The service configuration form appears.

12 Perform one of the following:

- a On the service navigation tree:
  - i Click on the plus sign (+) next to the Sites icon to show the sites in the service.
  - ii Right-click on the site(s) you want to move to another service and choose Move to Another Service from the contextual menu. A message appears.
  - iii Click Yes to continue. The Select Services form appears and displays a list of applicable services to which you can move the selected site(s).
- b On the service configuration form:
  - i Click on the Sites tab button to show the sites in the service.
  - ii Select the site(s) you want to move to another service and click on the Move to Another Service button. A message appears.
  - iii Click Yes to continue. The Select Services form appears and displays a list of applicable services to which you can move the selected site(s).

13 Select the required service and click the OK button. A progress message is displayed, followed by a confirmation message, once the move is complete.

14 Click the OK button.

15 Close the service configuration form.

Procedure 67-7 To delete customers

Note — You cannot delete customers that have associated services.

1 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

2 Search for the customer that you want to delete. The search results are displayed in the bottom panel of the form.

3 Choose the customer from the list and click on the Delete button. A Confirm dialog box appears.

Caution — Removing a customer deletes all information associated with the customer. Ensure that the correct customer has been selected.

4 Perform one of the following:

a Click on the No button to avoid deleting the customer. The Confirm dialog box closes.

b Click on the Yes button. The customer is deleted from the 5620 SAM database.

68 — Residential subscriber management

68.1 Residential subscriber management overview

The emergence of residential broadband networks and the availability of multiple service offerings, such as triple play applications create a requirement for greater service differentiation and control at the level of the individual service recipient. The 5620 SAM provides functionality for the efficient provisioning of access, QoS, and security features on IES, VPLS, and VPRN for residential subscribers, while service-level customization for end users is available using systems such as the Alcatel-Lucent 5750 SSC.

In the context of the 5620 SAM, a residential subscriber, sometimes called a subscriber, is a unique identifier that associates a group of end-user devices with policies. A subscriber can be associated with multiple SAPs on multiple NEs, and a customer can be associated with multiple subscribers.

A subscriber host, sometimes called a host, is an end-user device, such as a computer, VoIP telephone, or set-top box, that connects to the provider network and receives the service traffic. Hosts with the same subscriber identifier share overall HQoS and accounting characteristics as defined in a customer SLA, but may use QoS policies and queues that differ by the type and class of service offering.

Residential subscriber management supports service delivery models in a routed or bridged configuration, such as one VLAN per host, one VLAN per application, one VLAN for all applications, and one VLAN per service provider per application.

Residential subscriber configuration

The 5620 SAM supports the creation and configuration of residential subscriber management components using configuration forms. Configuring residential subscriber management on the 5620 SAM involves the creation and configuration of the following components, depending on the service delivery model:

- subscriber identification policies
- subscriber profiles
- SLA profiles
- subscriber explicit map entries
- ANCP policies
- PPPoE policies
- MSAP policies
- host tracking policies
- category map policies
- credit control policies
- IGMP policies
- BGP peering policies
- diameter policies
- subscriber multicast CAC policies

For detailed NE-specific residential subscriber management information, see the *7450 ESS OS Triple Play Guide* and the *7750 SR OS Triple Play Guide*.

A host requires subscriber-profile and SLA-profile associations to gain access to the network. Profiles define service attributes for hosts such as scheduling, accounting, security, and traffic prioritization by application type. A profile uses existing 5620 SAM policy definitions and allows the customization of policy parameters using override values.

A 5620 SAM user that is assigned the administrator, subscriber management, service management, or policy management scope of command role can perform all residential subscriber management functions, such as managing profile or DHCP-lease information.

The 5620 SAM allows the configuration of multiple components in one operation, but limits configuration to those parameters that are not specific to a component. For example, when a policy is applied to multiple profiles, the 5620 SAM removes pre-existing policy override values in the profiles.

Migrating to the TPSDA model

The following residential subscriber management functionality facilitates the migration of hosts from SAP-based aggregation to the TPSDA model. You can:

- Associate a subscriber with a SAP by using the SAP identifier as the subscriber identification string. The existing hosts on a SAP can then be automatically associated with a subscriber.
- Rename a subscriber. This changes the subscriber identification string for all hosts and facilitates a move from a default subscriber identification string to a string that complies with a particular naming scheme.
- Configure an intermediate destination identifier, such as a DSLAM name, for a static host and obtain the identifier from the Option 82 information in a DHCP packet. This functionality enables the listing of the hosts for a specific DSLAM and facilitates interworking with other TISPAN components such as the 5750 SSC.
- Configure a default subscriber identification string for the hosts on a SAP. This enables residential subscriber management functionality without the use of a subscriber identification policy or RADIUS authentication. This default string is associated with hosts when a string is not available from another source.
- Interpret an SLA profile string or subscriber profile string from a host as the profile name when a profile with a matching profile string is not found. This eliminates the need to map a profile string to a profile.

Configuration requirements

The following must be true before you can enable residential subscriber management on a SAP or deploy a profile to an NE.

- The NE must be a 7450 ESS, 7750 SR, or 7710 SR.
- For dynamic hosts on the SAP:
    - DHCP snooping is enabled on the upstream SAP or SDP.
    - For IES, DHCP relay is enabled on the downstream SAP.
- The NE has sufficient resources for creating the SLA profile instances, queues, and schedulers.
- For new or existing static hosts on the SAP:
    - Anti-spoofing on the SAP is configured with at least IP matching criteria.
    - A subscriber identification string is assigned.
    - A subscriber profile is assigned.
    - An SLA profile is assigned.
    - An IP address is assigned.

Functional description

When residential subscriber management on a SAP is enabled, a dynamic or static subscriber host that connects to the SAP requires a subscriber identification string to associate the host with a subscriber instance on the NE, or network access is denied. A subscriber identification string uniquely identifies a subscriber in the 5620 SAM.

You cannot delete an active component of a residential subscriber management configuration.

Enabling residential subscriber management on a SAP does not affect an existing dynamic host on a SAP until the host DHCP lease expires, at which point a subscriber identification policy manages lease renewal. Static hosts require the provisioning of a subscriber identification string for continued network access.

The 5620 SAM identifies the subscriber for a dynamic host by obtaining a subscriber identification string from a source such as the following:

- information that the host passes in the Option 82 field of a DHCP packet
- a RADIUS server
- the local user database

A static host requires explicit provisioning on the 5620 SAM that includes the association of a subscriber identification string.

You can optionally specify a default subscriber identification string for a SAP. You can enter the string or configure the 5620 SAM to use the SAP ID as the string.

The 5620 SAM deploys the components associated with a subscriber, such as policies and profiles, to an NE when one of the following occurs:

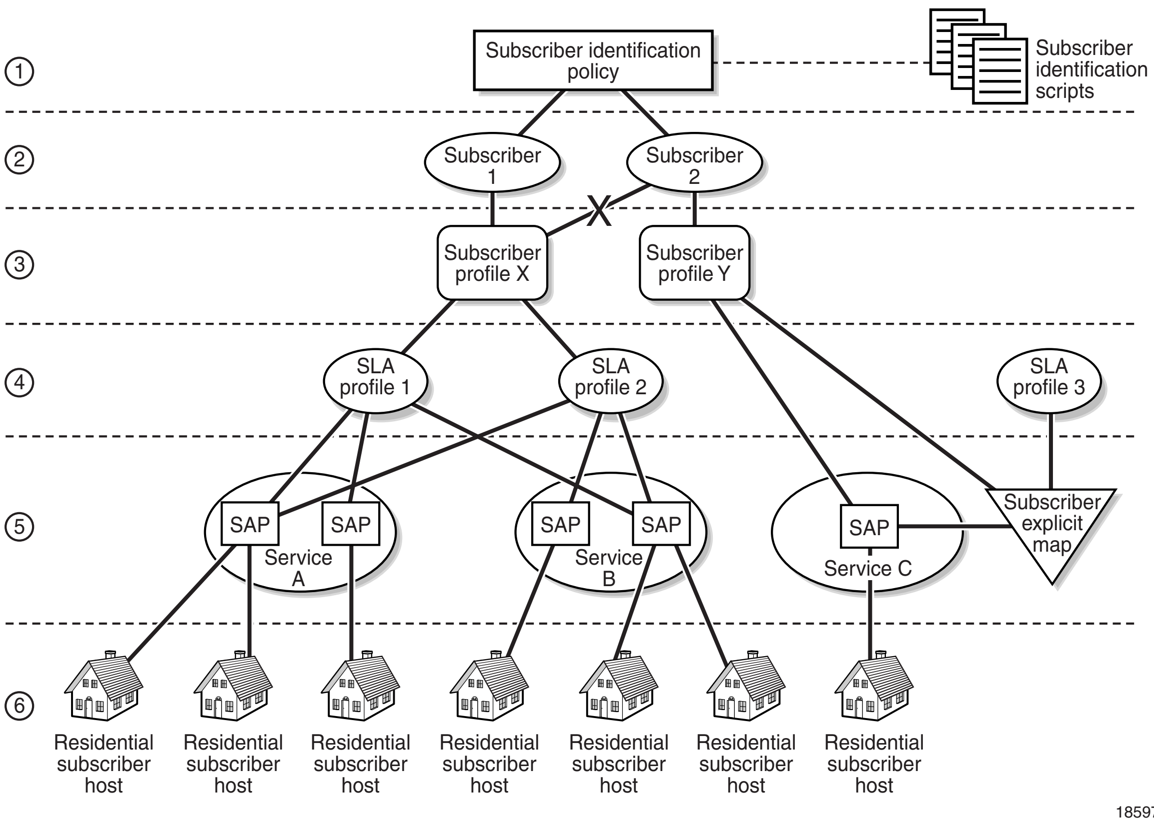
- The deployment of a subscriber identification policy with profile specifications
- The provisioning of the first static host for the subscriber on a SAP
- The provisioning of a Capture SAP with an MSAP Policy to automatically create an MSAP; see Managed SAP (MSAP) for more information

After the 5620 SAM deploys the subscriber and SLA profiles, the NE creates the queues, ACL filters and HQoS schedulers specified in the profiles. The NE ignores pre-existing queue or ACL filter policies on a SAP when subscriber management is enabled on the SAP.

The 5620 SAM maintains a record of subscribers that are deleted at the NE. Disconnected subscribers are marked as inactive. Subscriber information is retained in an inactive state in the Residential Subscriber and Residential Subscriber Instance views. In this way, the 5620 SAM treats the setup and teardown of a residential subscriber simply as a change of state, thereby avoiding the load imposed by object creation and deletion.

Figure 68-1 shows a conceptual model of the main component relationships in residential subscriber management. The model does not represent a specific type of service or service delivery mechanism and does not show all possible component configurations.

Figure 68-1 Residential subscriber management component relationships



As shown in Figure 68-1, there is a one-to-one relationship between a subscriber and a subscriber profile and a many-to-many relationship between subscriber profiles and SLA profiles. A subscriber profile or an SLA profile can apply to multiple SAPs or NEs, and can be specified as the default profile for the SAP or the NE.

Table 68-1 lists where to find configuration information for the components shown in Figure 68-1. The numbered levels segregate components for clarity only.

Table 68-1 Residential subscriber management components

Level	Component	Description	For more information, see	Procedure
1	Subscriber identification policy	Associates a dynamic host with a subscriber	"Subscriber identification policies" in this section	68-1
	Subscriber identification script	Parses DHCP Option 82 field to extract subscriber identification for a host, and optional profile, ANCP, and intermediate destination identification strings.	"Subscriber identification policies" in this section	68-47
2	Subscriber	Unique identifier that associates a group of subscriber hosts with policies	"Residential subscriber management overview" in this chapter	68-41

(1 of 2)

Level	Component	Description	For more information, see	Procedure
2	Subscriber instance	An instantiation of a subscriber on an NE	"Residential subscriber management overview" in this chapter	68-42
3	Subscriber profile	Names existing ingress and egress scheduler policies and an accounting policy for use by all hosts of a subscriber	"Subscriber profiles" in this section	68-14
4	SLA profile	Names existing QoS policies to define the traffic shaping for different classes of service within an application such as HSI, VoIP, VoD, or BTV Names existing ACL policies to filter the ingress and egress traffic	"SLA profiles" in this section	68-13
5	Subscriber explicit map	Lists subscriber identifiers and the associated SLA and subscriber profiles	"Subscriber explicit maps" in this section	68-34
6	Residential subscriber host (static)	A device such as a computer or set-top box that receives service traffic using a fixed IP address	"Static hosts and residential subscriber management" in this section	68-17 71-1, 73-1, and 74-1 access interface anti-spoofing configuration steps
	Residential subscriber host (dynamic)	A device such as a computer or set-top box that receives the service traffic using a temporarily assigned IP address	"Subscriber identification policies", "Subscriber profiles", "SLA profiles", "Subscriber explicit maps", Managed SAP (MSAP), and "PPPoE policies" in this section	68-43
5	Local DHCP server and PPPoE group interface	A local user database is created and associated to a local DHCP server and PPPoE group interface configuration	"Local DHCP servers" in this section	68-3 68-32 74-1 73-8

(2 of 2)

The 5620 SAM treats residential subscriber management components like policies. Depending on the distribution mode configuration of a local instance, when you modify a global component using the 5620 SAM, all local instances of the residential subscriber management component on the associated NEs can be updated. The Local Definitions tab of a component management form lists the local instances of the component.

Global residential subscriber management components are created in draft mode. This allows operators to verify the configuration before they distribute it to the network elements. See chapter 46 for information about global and local policy instances and policy distribution modes.

The maximum number of subscribers that use a SAP is configurable. When a SAP is limited to one subscriber, you can specify the treatment of traffic that does not match the subscriber profile, such as BTV traffic, which uses an IP address in the multicast range as the destination address. During single-subscriber SAP configuration, the 5620 SAM operator specifies whether to allow non-profile traffic and specifies the SLA and subscriber profiles to use for non-profile traffic, if it is allowed.

The 5620 SAM supports the collection of accounting statistics for subscriber instances. The 5620 SAM uniquely identifies a subscriber instance by using a combination of the subscriber identifier and the NE identifier.

Subscriber identification policies

Subscriber identification policies apply to SAPs and associate dynamic residential subscriber hosts with NE subscriber instances. Hosts that use the same subscriber identifier, called a subscriber identification string, belong to the same subscriber and receive common general HQoS and accounting treatment as defined by the customer SLA specifications in a subscriber profile. Hosts from multiple SAPs can belong to the same subscriber, but for HQoS scheduling purposes, all hosts of a subscriber must be active on the same IOM.

When a dynamic residential subscriber host requests an IP address using DHCP, the host can include a subscriber ID string and optional profile ID strings in the Option 82 field of the DHCP packet. If the request is approved by a DHCP server, the NE obtains the subscriber ID string for the host from the Option 82 information in the returning ACK message. The subscriber ID string is a match criterion for the assignment of SLA and subscriber profiles to the host unless profile ID strings are explicitly encoded in the DHCP option information by the host or configured as SAP default profiles. You can also configure a default subscriber ID string on a SAP.

Note — If adding Option 82 information to a DHCP relay packet causes the packet to exceed the DHCP relay maximum of 1500 bytes, the NE forwards the DHCP request without the Option 82 information. For this reason, short strings can be used as aliases for profile names.

A subscriber identification policy includes:

- URLs for subscriber identification scripts
- subscriber profile map
- SLA profile map

Entries in the subscriber and SLA profile maps are optional and are used for the direct assignment of profiles to hosts when hosts include profile ID strings in the DHCP Option 82 field.

Although the 5620 SAM is installed with no default subscriber identification policy, an operator can create a subscriber identification policy and designate it as the default policy by giving it the case-sensitive name “default”.

Subscriber identification scripts

A URL in a subscriber identification policy points to the location of a subscriber identification script that an NE uses to parse DHCP option information. During initialization, an NE downloads scripts from the URLs that are specified in the applied subscriber identification policies. An NE can store a maximum of four subscriber identification policies; each policy can contain up to three scripts.

A subscriber identification script derives the mandatory subscriber ID string, as well as a DSLAM identifier and optional profile ID strings, from the DHCP option information.

The 5620 SAM operator assigns a priority to each script in a subscriber identification policy. Only the operationally enabled script with the highest priority is active. If an NE encounters an error in a script or cannot find a script at the specified location, the NE marks the URL as operationally down, raises an alarm, and attempts to use the script that is next in priority. The script-related alarms that the 5620 SAM raises against the local instance of a subscriber identification policy are:

- warning alarm when the primary URL is operationally up but a lower-priority URL is operationally down
- major alarm when the primary script is operationally down but one of the other scripts is operationally up
- critical alarm when all scripts are operationally down

A modification to a subscriber identification script or URL takes effect only after the URL is administratively disabled and then re-enabled, which causes an NE to reload the script. Replacing or modifying a subscriber identification script or a URL can be service-affecting if not done properly. To avoid a service disruption when you modify a subscriber identification script or URL, perform Procedure 68-47.

Local DHCP servers

5620 SAM supports configuring local DHCP servers on a 7750 SR, 7710 SR, and the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the local DHCP server.

- Subscriber aggregation using a single NE or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

ARP host

You can use the 5620 SAM to configure and retrieve ARP hosts on a 7750 SR. ARP hosts are a subtype of enhanced subscriber host objects. The creation of the object is triggered by the reception of ARP messages from end-user devices. ARP hosts can be configured as an alternative to DHCP subscriber hosts or PPPoE sessions.

ARP host configuration can be performed on VPLS and MVPLS L2 access interfaces, IES and VPRN group interfaces, and VPRN retailer subscriber interfaces. The configuration includes enabling the functionality, setting the maximum limit of hosts per SAP or interface, and setting the default authentication interval.The configuration must be performed in conjunction with other enhanced subscriber management configuration on these interfaces. ARP hosts can be retrieved from the VPLS, MVPLS, and IES or VPRN SAPs. ARP hosts can also reside on MSAPs.

You can retrieve ARP hosts from the Manage→Residential Subscribers menu option. The Manage Residential Subscribers form opens. See Procedure 68-40 for more information about the persistence and retrieval of subscriber hosts.

Local user database

The 5620 SAM supports configuring a local database on a 7750 SR, 7710 SR, and the 7450 ESS. The local user database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured, otherwise it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. Once a local user database is configured, it can be associated with a local DHCP server and PPPoE configuration on a group interface.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address will not be authenticated.

Subscriber profiles

A subscriber profile defines the aggregate HQoS and accounting characteristics for the hosts of a specific subscriber. During the creation of a subscriber profile, the 5620 SAM operator chooses ingress and egress scheduler policies that apply to all host queues of the subscriber. A subscriber profile permits the optional selection of SLA profiles to override the SLA profiles that are named in the subscriber identification policy.

A subscriber profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign a subscriber profile to a host:

- subscriber explicit map
- subscriber identification policy

A subscriber requires an association with one and only one subscriber profile. If no subscriber profile is associated with a subscriber ID string or explicitly specified by a host, and there is no available default subscriber profile on an NE or on a SAP, the NE rejects the host.

A subscriber profile can include associations to the following policy types:

- ingress scheduler
- egress scheduler
- accounting
- ANCP
- NAT
- host tracking

- RADIUS accounting
- SLA profile map
- ingress QoS
- egress QoS
- HSMDA packet byte offset override
- HSMDA queue override
- ingress and egress scheduler policy parameter overrides
- ingress and egress policer control
- ingress and egress policer control overrides

The 5620 SAM operator can define a default subscriber profile for an NE or a SAP by giving it the case-sensitive name “default” during profile creation. NE and SAP default subscriber profiles apply to hosts for which a subscriber profile is unspecified in the subscriber explicit map and subscriber identification policy.

SLA profiles

An SLA profile defines the resources that an NE assigns to a particular subset of subscriber hosts, such as VoIP telephones or BTV set-top boxes. These resources include network-access and ACL policies. An SLA profile also optionally defines the maximum number of hosts that use the profile and the action taken when the number of hosts reaches the maximum.

An SLA profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign an SLA profile to a host:

- subscriber explicit map
- subscriber profile
- subscriber identification policy

An SLA profile includes:

- access ingress policy association
- access egress policy association
- ingress IP ACL filter policy association
- egress IP ACL filter policy association
- host limit that specifies the maximum number of hosts that use the SLA profile
- access ingress and access egress policy parameter override values
- access ingress and access egress policer override values

The queues in the access ingress and egress policies of an SLA profile must use a scheduler from the scheduler policy in the subscriber profile as their parent scheduler. All hosts that use the SLA profile must be active on the same IOM. When an SLA profile does not name an access ingress or access egress policy, an NE uses the SAP default policy.

A 5620 SAM operator can define a default SLA profile for a SAP. A default SAP SLA profile applies only to hosts for which an SLA profile is unspecified in the subscriber explicit map, subscriber profile, and subscriber identification policy.

Managed SAP (MSAP)

The 5620 SAM enables the automatic creation of subscriber hosts on a shared SAP, for which the most secure model is one subscriber per SAP. In this model, each subscriber has a separate VLAN, and this requires complex configuration. Automatic SAP creation builds on the authentication mechanisms that an NE supports to provide an automatically created SAP for the one-subscriber-per-SAP model. The automatically created SAP is called a managed SAP, or MSAP.

You can use the 5620 SAM to configure a policy and a SAP template for automatic MSAP creation. Automatic MSAP creation is enabled after a Capture SAP is created. See "Automatic MSAP creation process" in this section for information about creating a Capture SAP.

When a Capture SAP is configured, triggering packets initiate RADIUS authentication, which provides a service context. The authentication and the service context for this request creates an MSAP. An MSAP behaves the same as a regular SAP, but the MSAP configuration is not editable. The MSAP configuration is not kept in the NE configuration file, but it can be maintained in a separate persistency file.

An MSAP remains active as long as there is at least one subscriber host on the MSAP. See "MSAP management" in this section for more information about managing an MSAP.

Note — MSAPs cannot be configured, but are reconciled by the 5620 SAM on the NE.

Although MSAPs are not configurable, a user with a Policy Management or Subscriber Management role can create, list, delete, or modify an MSAP policy to control how the parameters apply during MSAP creation. An MSAP policy must be created before you create a Capture SAP so that the policy can be added to the Capture SAP configuration. See Procedure 68-5 for information about creating an MSAP policy.

You can create a Capture SAP only in a VPLS. A Capture SAP can create MSAPs in the routed CO configuration of an IES or VPRN, and in a VPLS TPSDA configuration. IES and VPRN MSAPs are restricted to group interfaces.

An MSAP is typically used by only one subscriber. In an architecture that provides service access using a shared SAP, you can use automatic SAP creation to a limited extent to reduce the configuration required, and to allow multiple subscribers to share a SAP. However, if more than one subscriber is allowed and an MSAP has been defined by a host, the installation fails and raises an event if a new host installation attempts to change the MSAP policy.

MSAPs are supported in HA and dual-homing environments. In dual homing, the MSAP is synchronized with the other NE during MSAP creation. For both HA and dual-homing environments, each participating NE must use the same MSAP policy.

Automatic MSAP creation process

A Capture SAP must be defined to trigger the process that automatically creates an MSAP. A Capture SAP does not forward traffic.

The encapsulation type of a Capture SAP can be one of the following:

- dot1q—supports the parameter value 4095, which appears as an asterisk (*)
- QinQ—supports the parameter values 1 to 4095 for the outer encapsulation value and 4095 only for the inner encapsulation value
- LAG—supports the parameter values 1 to 4095

The Capture SAP is used if a more specific match for the dot1q or QinQ tags is not found.

Note 1 — Some providers use QinQ encapsulation to represent a service.sub or sub.service SAP. When configured, the full QinQ represents a subscriber.

Note 2 — Multiple leases for the same subscriber are allowed; however, only one MSAP policy is allowed. If an MSAP is defined by a host and a new host installation is attempting to change the policy, the installation fails and raises an event.

The Capture SAP is created in the same way as a regular SAP; however, you must change the SAP Sub Type parameter that appears on the General tab of the L2 Access Interface (Create) form from the default value of Regular to Capture. Capture SAP-specific configuration is performed on the Capture Access Interface tab of the L2 Access Interface (Create) form. In the Capture Access Interface tab you can configure the parameters and apply the PPPoE and MSAP policies that control MSAP creation.

You can create a Capture SAP on any VPLS service on an NE. MSAP creation can be configured to start on receipt of DHCP packets, PPPoE packets, ARP packets, or any combination of DHCP, PPPoE, and ARP packets. After you configure the Capture SAP, every DHCP packet, PPPoE packet, or ARP packet received on the SAP is sent to the CPM, which triggers RADIUS authentication to provide a service context. The MSAP is created in the specified service. Non-triggering packets captured by the Capture SAP are dropped. See Procedure 68-20 for information about how to create a Capture SAP.

The following triggers are supported to initiate MSAP creation:

- DHCP Trigger Packets—DHCP Discover (or Requests if configured) for DHCP clients; the MSAP lifetime is defined by the lease time.
- PPPoE Trigger Packets—PPPoE PADI for PPPoE client; the managed SAP lifetime is defined by the session time. The MSAP is installed after an IP address is provided.
- ARP Trigger Packets—ARP for static-ip hosts; the MSAP lifetime is defined by ARP entry time. Current ARP entry refresh behavior is maintained.

If RADIUS does not provide all of the required information to install the host (for example, RADIUS lacks the IP address), the MSAP is created with a short timer while waiting for the host to be installed. Default SAP polices are available on the NE and will be used if the MSAP policy is not configured.

An MSAP is created with dual-pass (shared) queuing. The SLA profile of the host may change the queuing later in the process. The MSAP is always created with the default QoS and scheduling.

For MSAPs, the authentication policy is defined in the MSAP policy. Based on the configuration, the system reauthenticates the sessions when they are renewed. If the authentication policy is not used or when only PPPoE is used, the MSAPs, stay active when the session is renewed.

The authentication policy used in the Capture SAP must be the same policy as the policy used for the MSAP. For L3, the authentication policy is defined under the group-interface.

Note 1 — When PPPoE is used with MSAPs, the authentication policy must not use the username for MSAP creation.

Note 2 — The MSAP is not created (and an event is generated) if the group-interface name returned from RADIUS points to a different authentication policy than the policy defined by the Capture SAP.

MSAP management

MSAP management is applied using the MSAP policy. The MSAP policy is used to configure the parameters in the tabs that are available on the Properties forms of the MSAP. The original MSAP policy applied to the Capture SAP is the default Creation MSAP Policy, which is used to configure all of the parameters for the MSAP. You cannot modify an MSAP. However, you can modify the Creation MSAP Policy to make changes to an MSAP.

After MSAP creation, all of the MSAP parameters are read-only, except for the Creation MSAP Policy Re-evaluation parameter on the MSAP Properties tab. The Creation MSAP Policy Re-evaluation parameter allows you to reapply the MSAP policy associated with the local MSAP.

If you need to change an MSAP policy and you are in the Manage Subscriber Policy form, you can choose an MSAP policy, click on the Properties button, make your changes, and click on the Reevaluate MSAPs button to perform an MSAP policy re-evaluation. You can use the MSAP Policy Reevaluate button to update the MSAP policies on a global or local basis.

After an MSAP Policy Re-evaluate operation is performed on an MSAP, the MSAP form is not automatically updated with the new values. You must perform a resynchronization to update the parameter values. See Procedure 68-23 for more information about modifying and re-evaluating a Creation MSAP policy on an MSAP. See Procedure 68-24 for more information about modifying and re-evaluating an MSAP policy on one or more MSAPs.

Each MSAP can have one MSAP policy; however, the same MSAP policy can be applied to multiple MSAPs. The Capture L2 Access tab of the MSAP Policy form displays all of the Capture L2 access interfaces that are associated with this specific MSAP policy. You can change an MSAP policy locally or for all of the MSAPs that are associated with the MSAP policy. A change to a specific MSAP policy will cause the same change in all the MSAPs that use that policy if all of the MSAPs are re-evaluated or if the MSAP policy is re-evaluated.

Warning — If there is a disruption on the NE and the NE recovers by restarting, the MSAP policy that was changed and re-evaluated will be applied to all of the MSAPs associated to the policy.

The 5620 SAM treats the setup and teardown of MSAPs as state transitions to offset the load imposed by constant SAP creation and deletion. There are two states that an MSAP can have, active or inactive. These states cannot be configured. The state is automatically set to active when the MSAP is created on the NE. When the NE deletes the MSAP, the state changes to inactive. That is, when the MSAP is torn down, the state changes to inactive, the MSAP continues to be available in the 5620 SAM but is not used until it is reactivated by the NE. When the MSAP is reactivated, it will have the same identification so that the 5620 SAM can identify it with the same FDN.

The state information is not automatically updated in the 5620 SAM GUI. You must perform a resynchronization to retrieve the current state information. When the state is inactive, performance statistics for the MSAP are not retrievable; however, historical statistical records are available. You can schedule MSAP statistics or collect the statistics on demand. See the *5620 SAM Statistics Management Guide* for more information about scheduling and collecting statistics.

MSAPs are listed on the L2 Access Interface tab for VPLSs and on the Service Access Points tab of the IES and VPRN forms.

MSAPs are bound by the maximum number of SAPs allowed on the NE. Typically, and as long as services are not deleted, the number of MSAPs within the 5620 SAM are bound by the formula:

$$A \times B \times C$$

where:

A is the number of services

B is the maximum number of SAPs allowed on the NE

C is the number of NEs

Inactive services that previously contained MSAPs consume database space. MSAPs that have been in an inactive state for a long period of time or that are no longer used must be manually deleted. See Procedure 68-25 for more information about deleting an MSAP.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

MSAP alarm suppression

An IES or VPRN MSAP that is created on a LAG in an SRRP deployment uses a 5620 SAM mechanism to suppress unnecessary AccessInterfaceDown alarms. The mechanism uses the SRRP states of the redundant BNGs, and determines whether to raise the alarm based on the following rules:

- When the active BNG is in the master SRRP state and the standby BNG is in the initialize or backupShunt SRRP state, no AccessInterfaceDown alarm is raised against the standby BNG.
- If the standby BNG reboots, or if there is a link failure between the standby BNG and the access network, the MSAP AccessInterfaceDown alarms are suppressed for the standby BNG. The active BNG continues to remain in the master SRRP state. In this scenario, there may be other alarms on the standby BNG for card or link failures.
- After a fault that results in an SRRP failover, for example, active BNG reboot or loss of access network connectivity on the active BNG, an AccessInterfaceDown alarm is raised against each BNG. The alarms clear after SRRP state convergence.
- After a fault that affects both BNGs concurrently and disables SRRP redundancy, an AccessInterfaceDown alarm is raised against each BNG. The alarms clear when a BNG regains connectivity and assumes the role of SRRP master.

Note — The alarm-suppression mechanism can function correctly only when SRRP is correctly configured. If an SRRP peer is missing or disabled, the alarms may not be suppressed for the BNG that the 5620 SAM perceives to be the standby BNG.

MSAP event logs

An MSAP event log records the date, time, and active state for each state change that occurs after the MSAP is created. An event log is not recorded when the MSAP is created, although the information is recorded in a time stamp. You can view the event log for each MSAP, purge the event log records, and modify the global MSAP log policy retention time and administrative state.

MSAP time stamps

You can view the following MSAP state time stamps:

- date and time that the MSAP was created
- date and time of the last active state change

See Procedure 68-21 for information about viewing MSAP properties.

MSAP creation and management tasks

Table 68-2 summarizes the tasks required for MSAP creation and management.

Table 68-2 MSAP creation and management tasks

Task:	See:
Create an MSAP policy that will be added to a Capture SAP	Procedure 68-5
Create a Capture SAP that will enable creation of an MSAP	Procedure 68-20
List MSAPs	Procedure 68-21
View the event log for an MSAP, modify the global MSAP log policy, and purge the log records for an MSAP	Procedure 68-22
Modify and reapply an MSAP policy	Procedure 68-23
Modify and re-evaluate an MSAP policy on one or more MSAP	Procedure 68-24
Delete an MSAP to create more space	Procedure 68-25
Delete an MSAP policy	Procedure 68-26

Subscriber explicit maps

A subscriber explicit map is a table that directly associates dynamic subscriber hosts with subscriber profiles and SLA profiles. The entries in a subscriber explicit map override the default profile definitions. A subscriber ID string is the unique key for a subscriber explicit map entry.

A subscriber explicit map includes:

- subscriber ID string
- subscriber profile name
- SLA profile name
- AA group policy name
- subscriber ID alias

A subscriber explicit map does not allow the association of a subscriber ID string with the subscriber profile called “default”. However, if the explicit mapping omits a subscriber profile, the subscriber ID string is associated with the SAP or NE default subscriber profile. An attempt to delete a subscriber profile that is named in a subscriber explicit map fails. A 5620 SAM operator can remove explicit map entries at any time.

If an operator creates a subscriber explicit map entry without using the 5620 SAM, for example, using CLI, the 5620 SAM creates a subscriber instance in the global subscriber explicit map. If the 5620 SAM subsequently discovers another NE with the same subscriber entry that has a mapping to different profile, the 5620 SAM treats the second mapping as a local mismatch to the global entry for the subscriber.

Static hosts and residential subscriber management

Static subscriber hosts require explicit provisioning rather than an association with a subscriber identification policy. Static hosts for VPLS are configurable on the anti-spoofing tab of the L2 access interface management form. For IES and VPRN services, static hosts are configurable using the management form for a SAP on a group interface. Static host configuration involves the following elements:

- IP address
- MAC address (optional)
- subscriber ID string, or the use of the SAP ID as the subscriber ID
- valid subscriber profile
- valid SLA profile
- ANCP string
- intermediate destination, such as a DSLAM
- application profile

Note — When residential subscriber management is enabled on a VPLS SAP that is part of an operational MC ring group, the following must be configured on each static host:

- an intermediate destination that is a ring node in the MC ring group
- subscriber identification, such as a subscriber ID string or the use of the SAP ID as the subscriber ID
- a subscriber profile
- an SLA profile

ANCP policies

An ANCP policy defines the behavior of the residential subscriber host with which the policy is associated. An ANCP policy includes one of the following:

- static ANCP association
- static ANCP MSS association
- dynamic subscriber-profile association on VPLS, IES, VPRN and VLL services

An ANCP policy conveys status and control information based on port-up/port-down messages and changes to the current access line rate between the edge device and the access node. This allows the 7450 ESS, the 7750 SR, or the 7710 SR to adjust the HQoS subscriber scheduler with the correct rate or raises an alarm when the rate goes below a set threshold. The policy can be changed if the rate drops below a minimal threshold value. The ANCP actual upstream synchronization rate is configured in the ingress panel while the ANCP actual downstream synchronization rate is configured in the egress panel.

Host tracking policy

A host tracking policy is used to allow a subscriber's video traffic (multicast) to be included in the egress rate control for the subscriber. When a host tracking policy is specified in a subscriber profile, the egress traffic rate for the subscriber takes into account the unicast and multicast traffic in the aggregate egress rate or in the egress scheduler rate specified in the ANCP policy. There is no default host tracking policy.

When a host tracking policy is applied to a subscriber profile, all subscribers associated with the subscriber profile are tracked using that host tracking policy. You can view the tracked subscribers on the associated local host tracking policy property form.

You can also configure IGMP host tracking parameters on VPLS, IES, and VPRN service sites and SAPs.

The following on-demand host tracking information is available:

- on the Residential Subscriber Instance form, Host Tracking Info tab button, which hosts are being tracked for this particular subscriber
- on the Residential Subscriber Instance form, Host Tracking Status tab button, the egress traffic rate reduction for this particular subscriber
- on the VPLS L2 access interface property form, Host Tracking Info tab button, which hosts are being tracked
- on the IES and VPRN service access point property form, Host Tracking Info tab button, which hosts are being tracked

On-demand historical and real-time host tracking statistics are supported for SAPs and residential subscribers. Only historical statistical plotting is supported. The statistics and read-only host tracking information can be cleared by the 5620 SAM.

Diameter policies

The 5620 SAM supports diameter policies and associated diameter peers. Diameter policies are used in a subscriber management context to provide a credit control mechanism. The diameter policy establishes a server/peer configuration, as well as Diameter Credit-Control Application (DCCA) support. The NE functions as the credit control client, while the peer acts as the credit control server.

DCCA represents an alternative to RADIUS for providing a mechanism to support pre-paid service model in access networks. Under a DCCA configuration, the credit control server is used to grant service to a subscriber for pre-defined duration. Before a subscriber host is created, the BNG queries the credit control server about the credit for the given subscriber. If credit is granted, the subscriber host is installed with the appropriate SLA level. If the subscriber has no credit, the credit control server denies access and no subscriber host is created.

The diameter policy is used to specify common diameter protocol parameters, while the diameter peer defines the relationship with an external diameter server. The diameter protocol parameters defined on the diameter policy describe connection and session characteristics, and indicate which attribute-value pairs (AVPs) to use in messages.

Peers

The diameter policy defines a set of peers with which to establish diameter sessions. Peers share the configuration of the policy with which they are associated, but can override individual timer parameters inherited from the policy. In addition, each peer defines transport and connection-specific parameters, values for destination-specific AVPs, and a preference value.

The 7750 SR and 7450 ESS provide read-only operational values and statistics for the peer definition of local diameter policies. The 5620 SAM can provide a snapshot view of operational values and statistics. Operational values include the peer's timer values, the current state of the peer's state machine, and the peer's order among the other peers within the policy.

DCCA

The 7710 SR and 7750 SR support a DCCA, which can be customized through a set of parameters on the diameter policy in the 5620 SAM. The parameters allow customization of DCCA error handling, DCCA timer(s), and AVP value definitions.

PPPoE policies

PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. PPPoE takes advantage of the speed of a packet-based Ethernet network with the security and accounting functions of a PPP network. PPPoE allows service providers to use existing RADIUS authentication.

Since more than one subscriber is sharing the same connection to a service provider, PPPoE organizes subscribers during two stages:

- PPPoE discovery stage
- PPPoE session stage

During the discovery stage, the subscriber and service provider identify each other’s MAC address and establish a PPPoE session ID.

The PPPoE discovery stage consists of the following steps:

1. PPPoE Active Discovery Initiation (PADI). The client initiates a session by broadcasting a PADI packet to the LAN to request a service.
2. PPPoE Active Discovery Offer (PADO). Any access device that can deliver the service requested by PADI packet, replies with a PADO packet that contains its name, unicast address and service requested.
3. PPPoE Active Discovery Request (PADR).The client selects one of the PADOs that it receives and sends a PADR packet to indicate the services required.
4. PPPoE Active Discovery Session Confirmation (PADS). When the selected device receives the PADR packet, it can accept or reject the PPPoE session. To accept the session the device sends the client a PADS packet with a unique ID and a service name. If the device rejects the session, it sends a PADS packet with a service name error and resets the session ID to zero.

During the session stage, PPPoE behaves as a peer-to-peer protocol. Each PPPoE session is identified by the MAC address of the peer and the session ID. Once a session is established, both end points build a point to point connection over the Ethernet and exchange packets. Once the connect is established, the RADIUS accounting policy can begin. LCP negotiates authentication parameters. After a session is authenticated IPCP sends an IP address to the PPPoE client. IP Addresses can be stored in the DHCP local user database, if configured.

After a session is established both end points monitor the session and can terminate a session after a configured number of keep alive intervals are exceeded. An alarm is raised by the 5620 SAM when a PPPoE session fails. Either peer can send a PPPoE Active Discovery Termination (PADT) packet. See "Local DHCP servers" in this chapter for more information on associating PPPoE with a local DHCP server.

PPPoA sessions

PPPoA is used in subscriber networks to encapsulate PPP frames inside ATM Adaption Layer 5 packets. Each PPP session is carried over a single ATM VC to the BNG. Two types of encapsulation are supported:

- AAL5_nlpid_PPP
- AAL5_Mux_PPP

PPPoEoA sessions

PPPoEoA is used in subscriber networks to encapsulate PPPoE messaging within ATM Adaption Layer 5 packets. Each PPP session can be directly terminated on any host within the customer Ethernet network and then transported over an ATM network to the BNG. Two types of encapsulation are supported:

- AAL5_muxed_bridged_EHT_no_FCS
- AAL5_snap_bridged

Subscriber host connectivity verification

Aside from relatively infrequent IP-address lease renewal, DHCP has no session-monitoring or connection-monitoring capability. Residential subscriber management provides this functionality for DHCP hosts and static hosts using subscriber host connectivity verification, or SHCV.

When SHCV is enabled on a SAP, an NE issues a periodic ARP request to each host on the SAP. If the NE receives no reply to an ARP request within the specified interval, the NE raises an event. When SHCV is configured to drop a lost host, the NE immediately removes the host from its active subscriber host table.

SHCV records the state information that it collects for hosts on a SAP and maintains a history of connectivity-related events for troubleshooting purposes. The size of the history log is restricted by a size-constraint policy.

SHCV operates in conjunction with DHCP snooping and is configurable on VPLS, VPRN, and IES SAPs and on IES group interfaces. Because it uses ARP, SHCV automatically populates the FIBs of bridging devices in the access and provider networks. The configurable items for SHCV on a SAP include:

- frequency of connectivity checks
- source of the ARP request
- action to take when a host loses connectivity

Note — On an L2 access interface, SHCV uses the NE system IP address as the source of the ARP request. On an L3 access interface, SHCV uses the IP- and MAC-address combination of the interface or the VRRP state for the interface as the ARP source. On IES group interfaces, SHCV uses the address of the subscriber interface as the source.

The behavior that an NE exhibits toward SHCV events is configurable using the residential subscriber management form. The configurable NE SHCV items include:

- maximum host connectivity loss rate
- action to take when the connectivity loss rate exceeds the maximum
- action to take when the NE drops an event trap, as such an event may indicate a high connectivity loss rate

SHCV event handling on an NE is disabled by default. When SHCV is enabled on a SAP but is disabled on the NE, the 5620 SAM records the blocking of SHCV events in the SHCV log. This ensures that an operator is aware of SHCV activity when viewing the SHCV log, even if the NE is configured to suppress SHCV events.

The following conditions represent an SHCV host connectivity loss:

- absence of a host response
- inconsistency between the reply data and the DHCP lease state

An NE makes more than one SHCV attempt before it raises an event against a host to ensure that the absence of a host response indicates a host connectivity problem and is not simply the result of occasional packet loss.

When a SAP becomes operationally down, the NE generates one trap for the SAP rather than one trap for each host on the SAP. When the SAP returns to service, the NE forwards a trap for each host as it verifies the restoration of connectivity. SHCV generates the following event traps:

- SAP up
- SAP down
- host up
- host down
- trap dropped

Routed CO

A broadband access network typically requires the aggregation of the traffic from access equipment before routing of the traffic is possible. Routed CO functionality allows a network operator to directly connect a DSLAM or similar multiplexer to a router such as the 7750 SR. Residential subscriber management, combined with the use of DSCP or dot1p values, supports access-integration models such as the following:

- one SAP for all subscribers and service offerings
- one SAP per service offering
- one SAP per subscriber

Routed CO allows the configuration of subscriber interfaces and group interfaces on IES and VPRN. A subscriber interface defines the subnets that are available to a subscriber. A group interface is a child object of a subscriber interface that allows the configuration of multiple SAPs as part of a single interface. Routed CO functionality depends on residential subscriber management to maintain the subscriber host information.

The 5620 SAM supports routed CO in IES and VPRN services:

There is no direct association between the subnets and the group interfaces. Subnets can be shared between group interfaces. If the host IP address is not in one of the subnets, packets from the network to that host IP are not received by the subscriber or group interfaces.

A subscriber interface defines a maximum of 16 subscriber subnets and acts as the DHCP relay agent for a subscriber. For the forwarding of DHCP packets to a subscriber server, a subscriber interface requires the specification of a gateway address that is in one of the subscriber subnets. Group interfaces below the subscriber interface inherit this gateway address but can specify an override value if required.

All SAPs in a group interface use the same port. The first SAP on a group interface determines which port the group interface uses. Additional SAPs for the group interface must be associated with the group-interface port during SAP creation.

A group interface is similar to a regular IES interface except for the following.

- Multiple SAPs are configurable.
- No IP addresses are specified.
- No broadcast traffic is permitted.
- No loopback mode exists.
- No static ARP can be specified.
- VRRP is not supported.

When a subscriber interface or a group interface is operationally disabled, no packets are sent to or from the subscriber hosts on the SAPs of the interface, but the state information for a static or dynamic host persists until the static host is removed from the NE by an operator or the DHCP lease of the dynamic host expires.

Because the configuration of multiple SAPs on a group interface makes normal forwarding of DHCP responses to hosts impossible, DHCP relay for routed CO maintains a cache of DHCP requests. If a DHCP server response does not arrive within the specified interval time, the NE discards the cache entry. The 5620 SAM operator can choose to have the NE use the Option 82 circuit ID field in a DHCP request as the match criterion for the returning DHCP ACK message.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT for routed CO requires a NAT policy that is associated with a subscriber profile. In an IES routed CO deployment, NAT is configured on the base routing instance of an NE. NAT in a VPRN routed CO deployment is configured on the VPRN routing instance. See chapter 30 for general information about configuring and deploying NAT. See chapter 46 for information about configuring a NAT policy. See Procedure 68-14 for information about associating a NAT policy with a subscriber profile.

Lease populate is enabled on a group interface by default, and the number of allowable lease entries is set to one. All SAPs on the group interface inherit this configuration during creation.

See chapters 73 and 74 for more information on configuring subscriber and group interfaces for IES and VPRN services.

Wholesale and retail configurations for VPRN services

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. The implementation of configuration changes occurs as if the VPRN is a standalone router using the routed CO model. The benefit of this model is flexibility for the retailer and decreased involvement for the wholesaler.

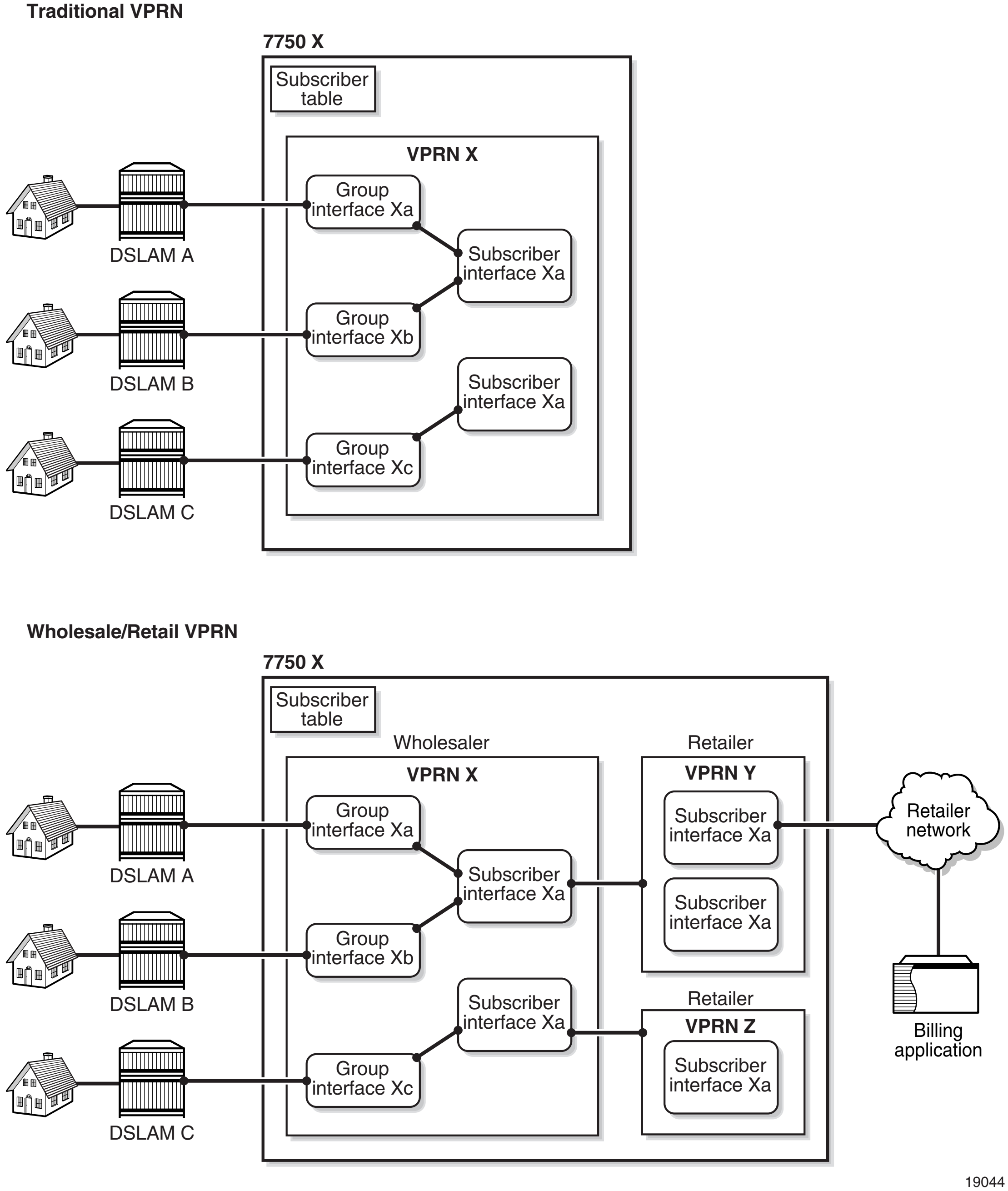
You must use a subscriber SAP to support shared access for multiple retailers. Another dependency of shared access is the requirement for the wholesaler to maintain separate access nodes for each retailer with network scaling issues.

In the wholesale and retail model, the wholesaler instance connections that are common to the access nodes are distributed to many retail instances. Upstream subscriber traffic ingresses into the wholesaler instance and, after identification, is then forwarded into the retail instance. The reverse principle occurs for traffic in the opposite direction. The wholesale and retail traffic flow is controlled with minimal communication to the RADIUS server. A RADIUS policy is defined in the wholesaler instance. The RADIUS response used during the subscriber instantiation provides the service context of the retailer VPRN. If the wholesaler has a retail business, the operator can configure a separate VPRN for their retail services.

The retailer subscriber interface primarily controls the DHCP configuration. The single exception to this model is the lease-populate value. The lease-populate value in the wholesale context controls the individual SAP limits. The lease-populate value in the retail subscriber interface controls the limits for that retailer interface. The wholesale and retail limits must be met before the instantiation of a new subscriber.

Figure 68-2 shows the configuration for a traditional and wholesale retail VPRN.

Figure 68-2 Routed CO for traditional and wholesale/retail VPRNs



See chapter 74 for more information on configuring the forwarding service component for wholesale and retail VPRN services.

Subscriber host polling and monitoring

Subscriber hosts can be periodically polled and monitored for certain DHCP event changes. A subscriber host monitoring configuration form is available from the Manage Residential Subscribers form.

The maximum number of hosts that can be selected for monitoring is configurable through XML; the default is five. Host monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Subscriber Host form displays a variety of polled information about the host that is obtained from the NE. You can also open a DHCP event log for the host from the Host Properties form. The logged events include information on DHCP lease renewals, lease expiration, and profile changes. An entry is added to the table whenever a new event occurs. You can purge event entries using the Host Properties form.

Host monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period and polling interval can be configured.

The Host monitored objects and associated events are stored in the 5620 SAM database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

SAP monitoring

You can monitor the DHCP events on one or more SAPs. A SAP monitoring form is available from the Manage Residential Subscribers form.

The maximum number of SAPs that can be selected for monitoring is configurable through XML; the default is five. SAP monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Access Interface form displays a variety of DHCP-related events or notifications about subscriber hosts on a SAP that are compiled using traps received from NEs. You can also open an event log for the SAP from the SAP Properties form. The logged events include information on DHCP lease entries, lease states, and host connectivity. An entry is added to the table whenever a new event occurs. You can purge event entries using the Monitoring Configuration form.

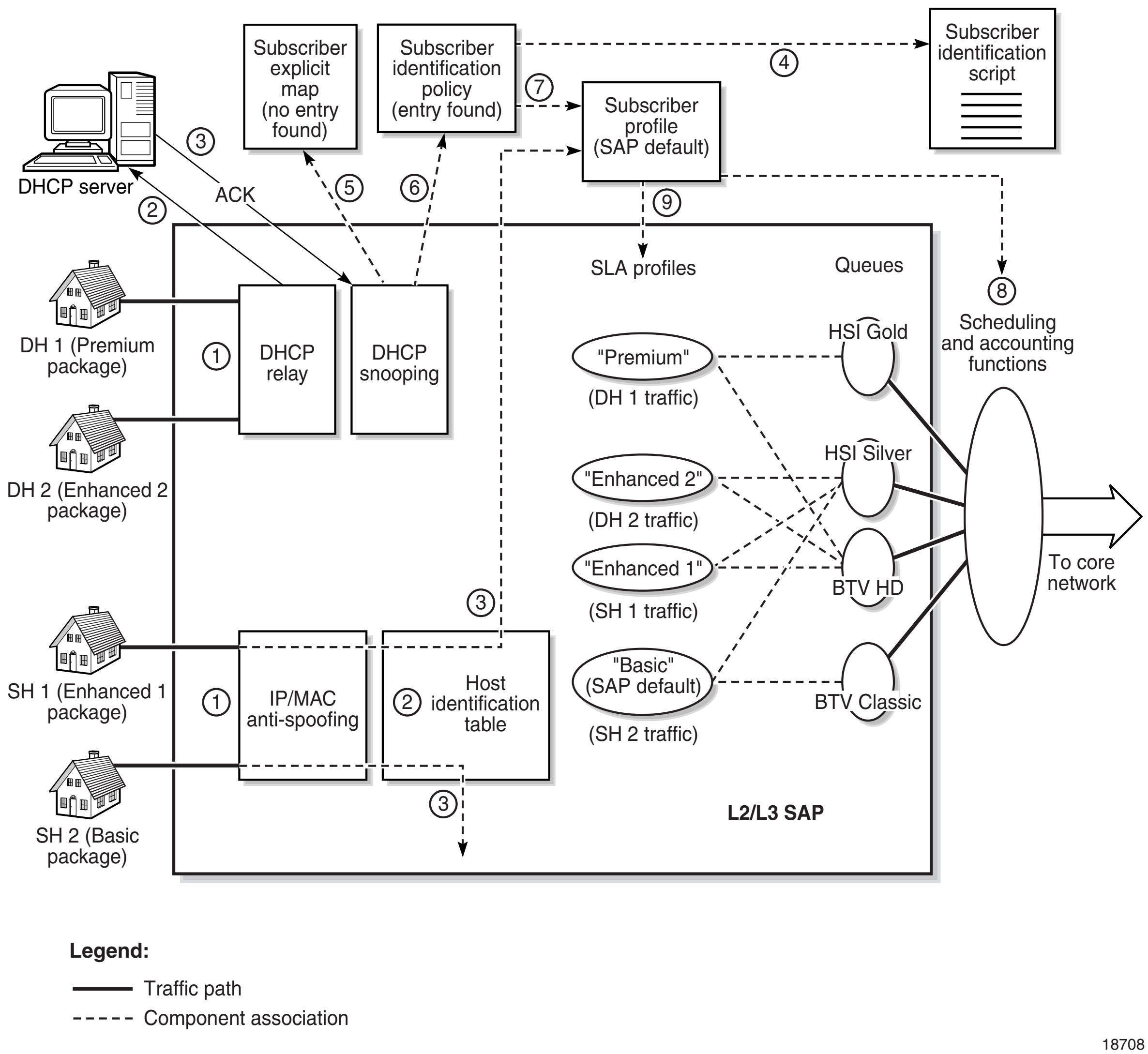
SAP monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period can be configured.

The SAP monitored objects and the associated events are stored in the database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

68.2 Sample configuration

Figure 68-3 shows how residential subscriber management assigns resources to dynamic and static hosts. Many different configurations are possible; the sample portrays the residential subscriber management mechanism rather than a particular service delivery model. For simplicity, the sample consists of one subscriber instance on one SAP, and two types of service offering. Each service offering is available in two classes.

Figure 68-3 Sample configuration



The customer provides a subscriber identification string, the names of the four end-user service packages, and the bandwidth and class requirements for each package. Each package is a combination of HSI and BTV. A 5620 SAM operator creates four queues and four SLA profiles with which the queues are associated, as shown in Table 68-3. Alcatel-Lucent recommends that the 5620 SAM operator give the SLA profiles the same names as the packages to prevent confusion.

Table 68-3 Sample configuration service packages

Subscriber host	Package name	SLA profile name	Associated queues
DH 1	Premium	Premium	HSI Gold, BTV HD
DH 2	Enhanced 2	Enhanced 2	HSI Silver, BTV HD

(1 of 2)

Subscriber host	Package name	SLA profile name	Associated queues
SH 1	Enhanced 1	Enhanced 1	HSI Gold, BTV Classic
SH 2	Basic	Basic	HSI Silver, BTV Classic

(2 of 2)

The customer offers two classes of BTV and HSI services:

- BTV HD: high-definition broadcast television
- BTV Classic: regular-definition broadcast television
- HSI Gold: high-bandwidth broadband Internet access
- HSI Silver: regular broadband Internet access

The following steps, which correspond to the numeric labels in the upper part of Figure 68-3, define the sequence of events for dynamic subscriber hosts that attempt to join the network.

1 Dynamic Host 1 (DH 2) and Dynamic Host 2 (DH 2) each send a DHCP request to the SAP.

2 DHCP relay on the SAP forwards the DHCP requests to the DHCP server.

3 The DHCP server authorizes the requests and responds with a DHCP ACK message for each subscriber host.

4 The subscriber identification policy uses a script to obtain the subscriber identification string, an optional subscriber profile string, and an optional SLA profile string from the Option 82 information in each ACK message. DH 1 and DH 2 provide the same subscriber profile identification string but different SLA profile strings.

5 The NE checks the subscriber identification string values against the entries in the subscriber explicit map and finds no matching entries for the hosts.

6 The NE checks the subscriber profile string and the SLA profile string values for each host against the subscriber identification policy.

7 The NE assigns the same subscriber profile to DH 1 and DH 2 based on the subscriber profile string provided by each host.

8 DH 1 is the first host to join the network, so the scheduling and accounting functions associated with the assigned subscriber profile are instantiated on the SAP.

9 The NE matches the SLA profile string provided by each host to an SLA profile. The NE assigns the Premium SLA profile to DH 1 and the Enhanced 2 SLA profile to DH 2 based on the provided SLA profile strings. These are the first hosts of the subscriber to join the network, so the appropriate queues are instantiated on the SAP based on the SLA profile specifications, and host traffic subsequently flows.

The following steps, which correspond to the numeric labels in the lower part of Figure 68-3, define the sequence of operations for static subscriber hosts that join the network.

1 Static Host 1 (SH 1) turns on the computer, and Static Host 2 (SH 2) turns on the television.

2 The host devices request network access; IP- matching (and optional MAC-matching) anti-spoofing on the SAP checks the static host table on the NE and validates both requests.

3 The NE assigns resources to each static host based on subscriber profile and SLA profile designations, and host traffic subsequently flows.

- The static host table entry for SH1 names a subscriber profile and an SLA profile. Although SH 1 is the first host to use this SLA profile, the queues defined in the profile are already instantiated because of the application of the SLA profiles for DH 1 and DH 2.
- For SH 2, there is no explicit association between the host and a subscriber profile or an SLA profile, so the NE assigns the SAP default subscriber and SLA profiles, which define the most basic service package the customer offers to end users.

68.3 Workflow to manage residential subscribers

1 Create a service that effectively delivers the proposed residential service offering. See Chapter 64 for more information.

2 Depending on your service delivery model, configure the following policies as required:

- subscriber identification policy. See Procedure 68-1.
- ANCP policy. See Procedure 68-2.
- PPPoE policy. See Procedure 68-3.
- PPP policy. See Procedure 68-4.
- MSAP policy. See Procedure 68-5
- host tracking policy. See Procedure 68-6.
- category map policy. See Procedure 68-7.
- credit control policy. See Procedure 68-8
- IGMP policy. See Procedure 68-9.
- BGP Peering policy. See Procedure 68-10
- diameter policy. See Procedure 68-11.
- subscriber multicast CAC policy. See Procedure 68-12.

3 Create ingress and egress scheduler policies for the subscriber hosts in accordance with the customer SLA. See Procedure 47-15.

4 Create an accounting policy for the customer. See the *5620 SAM Statistics Management Guide* for more information.

5 Create access ingress and access egress QoS policies for the different applications, for example, HSI and VoIP, and levels of service, for example, gold, silver, and bronze, that subscriber hosts are to receive. See Procedure 47-1 and 47-3. Associate the queues in the QoS policies with the previously created ingress and egress scheduler policies.

6 Specify a unique subscriber identification string for the subscriber, according to your customer specifications. See “Functional description” in this chapter for the different options for specifying a subscriber identification string.

7 Create a RADIUS-based accounting policy for the subscriber, as required. See Procedure 53-1.

8 Create a policer control policy for the subscriber, as required. See Procedure 47-20.

9 Create SLA profiles that name the previously created QoS policies. See procedure 68-13 for more information.

- **i** Create a different SLA profile for each class of service offering.
- **ii** Use override values to customize the policy values, as required.
- **iii** Use override values to customize the policer values, as required.

10 Create a subscriber profile. See procedure 68-14 for more information.

- **i** Choose the previously created ingress and egress scheduler policies.
- **ii** Choose the previously created accounting policy.
- **iii** Enable accounting.
- **iv** Assign the previously created RADIUS-based accounting policy, as required.
- **v** Assign the previously created ingress and egress policer control policies, as required.
- **vi** Associate one or more of the previously created SLA profiles with the subscriber profile.

11 Create, configure, and manage SAPs, as required.

- **a** Assign the subscriber profile and SLA profiles to the service SAPs. See Procedure 68-15.
- **b** Enable or disable residential subscriber management on a SAP. See Procedure 68-16.
- **c** Specify a subscriber identifier, subscriber profile, and SLA profile for each static host, as required, if default values are not configured on the SAP. See procedure 68-17 for more information.
- **d** Configure a MEP on a SAP. See Procedure 68-18.
- **e** List and manage subscriber management SAPs. See Procedure 68-19.

12 Create, configure, and manage MSAPs, as required.

- **a** Create a Capture SAP that will enable the creation of an MSAP. See Procedure 68-20.
- **b** List MSAPs and view MSAP properties. See Procedure 68-21.
- **c** View an MSAP event log, modify the global MSAP log policy, and purge MSAP log records. See Procedure 68-22.
- **d** Modify and re-evaluate an MSAP policy on an MSAP. See Procedure 68-23.
- **e** Modify an MSAP policy and re-evaluate the MSAPs. See Procedure 68-24.

f Delete an MSAP. See Procedure 68-25.

g Delete an MSAP policy. See Procedure 68-26.

13 Configure or monitor DHCP or NE SHCV events or databases, as required.

a Configure DHCP event monitoring for a SAP. See Procedure 68-27.

b Monitor DHCP events for a SAP. See Procedure 68-28.

c Configure DHCP lease management for a subscriber host. See Procedure 68-29.

d Configure DHCP event monitoring for a subscriber host. See Procedure 68-30.

e Monitor DHCP events for a subscriber host. See Procedure 68-31.

f Configure a local user database to authenticate DHCP clients. See Procedure 68-32.

g Configure NE SHCV event handling. See Procedure 68-33.

14 Turn up the service.

15 Provide the customer with the necessary IP information for provisioning dynamic and static hosts in the customer network.

16 Perform one or more of the following, as required.

a Create a subscriber explicit map, if required. See procedure 68-34 for more information.

b Retrieve PPPoA sessions. See Procedure 68-35.

c Configure a MEP on an SDP Binding. See Procedure 68-36.

d Configure L2Aware static port forwarding on a residential subscriber instance. See Procedure 68-37.

e Resynchronize static port forwarding entries. See Procedure 68-38.

f Collect, view, and clear host tracking statistics and information. See Procedure 68-39.

17 View information associated with the residential subscriber, as required.

a View subscriber host information. See Procedure 68-40.

b View a subscriber and the associated subscriber hosts. See Procedure 68-41.

c View a subscriber instance and the associated subscriber hosts. See Procedure 68-42.

- **d** View or configure active residential subscriber hosts on a SAP. See Procedure 68-43.
- **e** View SHCV log events. See Procedure 68-44.

18 Modify a subscriber's subscription details, as required.

- **a** Rename a subscriber. See Procedure 68-45.
- **b** Reset a subscriber's subscription credit limit. See Procedure 68-46.
- **c** Modify the primary subscriber identification script or URL. See Procedure 68-47.
- **d** Delete an inactive residential subscriber instance. See Procedure 68-48.

68.4 Residential subscriber management procedures

Use the following procedures to perform residential subscriber management tasks.

Procedure 68-1 To create or modify a subscriber identification policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

- **a** Create a subscriber identification policy.
  - **i** Click on the Create button and choose Create Subscriber Identification Policy from the drop-down menu. The Subscriber Identification Policy (Create) form opens.
  - **ii** Go to step 3.
- **b** Modify a subscriber identification policy.

  Caution — Modifying an active subscriber identification policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber identification policy before you proceed.

  - **i** Choose Subscriber Identification Policy from the object drop-down list.
  - **ii** Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.
  - **iii** Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Strings From Option
- Primary Script URL
- Primary Script Administrative State
- Secondary Script URL
- Remove oldest Subscriber Host
- Tertiary Script URL
- Tertiary Script Administrative State

Note 1 — You can designate a subscriber identification policy as the default policy by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber identification policy creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Supported Service Models tab button to indicate the intended service model for the subscriber identification policy.

Note — The 5750 SSC requires the specification of a service model for proper interoperation with the 5620 SAM.

5 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Bridged)

6 Click on the SLA Profiles tab button. The General tab is displayed.

7 Configure the Use Direct Map as Default parameter.

8 Perform one of the following steps to configure SLA profiles for the subscriber identification policy, if required.

a Assign an SLA profile.

i Click on the Create button. The SLAProfileEntry (Create) form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry (Create) form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

- v Click on the OK button to close the SLAProfileEntry (Create) form. A dialog box appears.
- vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the SLA profile entry.

b Remove an SLA profile.

- i Select an SLA profile and click on the Delete button. A dialog box appears.
- ii Click on the OK button. The SLA profile is removed from the list.
- iii If you want to assign an SLA profile to replace the removed SLA profile, go to step 8 a.

9 Click on the Subscriber Profiles tab button. The General tab is displayed.

10 Configure the Use Direct Map as Default parameter.

11 Perform one of the following steps to configure subscriber profiles for the subscriber identification policy, if required.

a Add a subscriber profile.

- i Click on the Create button. The SubscrProfileEntry (Create) form opens.
- ii Click on the Select button to choose a subscriber profile. The Select Subscriber Profile form opens.
- iii Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the SubscrProfileEntry (Create) form refreshes with the subscriber profile information.
- iv Configure the Subscriber ID Alias parameter.
- v Click on the OK button to close the SubscrProfileEntry (Create) form. A dialog box appears.
- vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the subscriber profile entry.

b Remove a subscriber profile.

- i Select a subscriber profile and click on the Delete button. A dialog box appears.
- ii Click on the OK button. The subscriber profile is removed from the list.

12 Click on the Application Profiles tab button. The General tab is displayed.

13 Configure the Use Direct Map as Default parameter.

14 Perform one of the following steps to configure application profiles for the subscriber identification policy, if required.

a Add an application profile.

i Click on the Create button. The AppProfileEntry (Create) form opens.

ii Click on the Select button to choose an application profile. The Select Application Profile form opens.

Note 1 — If the subscriber identification policy opened in step 2 is a global policy, global AA group policies are listed. If the subscriber identification policy is a local policy, local AA group policies are listed.

Note 2 — The global AA group policies must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 3 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

iii Select an application profile and click on the OK button. The Select Application Profile form closes, and the AppProfileEntry (Create) form refreshes with the application profile information.

iv Configure the Application Profile parameter.

v Click on the OK button to close the AppProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the application profile entry.

b Remove an application profile.

i Select an application profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The application profile is removed from the list.

15 Click on the OK button to close the Subscriber Identification Policy (Create) form. A dialog box appears.

16 Click on the Yes button. The Subscriber Identification Policy (Create) form closes.

17 Close the Manage Subscriber Policies form.

Procedure 68-2 To create or modify an ANCP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following:

a Create an ANCP policy.

i Click on the Create button and choose Create ANCP Policy from the drop-down menu. The ANCP (Create) form opens.

ii Go to step 3.

b Modify an ANCP policy.

i Choose an ANCP policy from the object drop-down list of the Manage Subscriber Policies form.

ii Configure the filter criteria and click on the Search button. A list of ANCP policies appears.

iii Select an ANCP policy and click on the Properties button. The ANCP Policy (Edit) form opens.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the following parameters in the Ingress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor (kbps)
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

  The Rate Modification Scheduler parameter is configurable when the Rate Modification parameter is set to Scheduler.

5 Configure the following parameters in the Egress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor Notification
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

  The Rate Modification Scheduler parameter is configurable when the Rate Modification Modification parameter is set to Scheduler.

6 Configure the following parameters in the Port Down panel:

- Disable SHCV
- Disable SHCV Notification
- Disable SHCV Hold Time (seconds)

7 Click on the OK button to close the ANCP Policy (Create) form.

Procedure 68-3 To create or modify a PPPoE policy

The 5620 SAM supports PPPoE configuration on the 7750 SR and the 7710 SR.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose PPPoE Policy (pppoe) from the object drop-down list in the Manage Subscriber Policies form.

3 Perform one of the following:

a Create a PPPoE policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create PPPoE Policy. The PPPoE Policy, Global Policy (Create) form opens.

b Modify a PPPoE policy.

i Configure the filter criteria and click on the Search button. A list of PPPoE policies appears.

ii Select a PPPoE policy and click on the Properties button. The PPPoE Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- PPP MTU
- LCP Keep-Alive Interval (seconds)
- LCP Keep-Alive Hold Up Multiplier
- Disable AC Cookies
- PADO Delay (100’s of milliseconds)
- Maximum Sessions Per MAC
- Enable Reply On PADT
- Authentication Type
- Minimum CHAP Challenge Length
- Maximum CHAP Challenge Length
- Initial Delay
- IPCP Subnet Negotiation

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The PPPoE Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 46-1 for more information about distributing a policy.

7 Click on the Options tab. A list of options appears.

8 Perform one of the following:

a To add an option, go to step 12.

b To edit an existing option, go to step 9.

9 Choose an option from the list.

10 Click on the Properties button. The PPPoE Option (Edit) form opens.

11 Go to step 13.

12 Click on the Create button. The PPPoE Option (Create) form opens.

13 Configure the parameters:

- Option Protocol
- Custom Option Number
- Option Type
- Option Value
- IP Address

14 Click on the OK button to close the PPPoE Option (Create) form. A dialog box appears.

15 Click on the OK button. The PPPoE Option (Create) form closes.

Procedure 68-4 To create or modify a PPP policy

The 5620 SAM supports PPP configuration on the 7450 ESS, 7750 SR, and the 7710 SR, release 4 and later.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose PPP Policy (PPP Policy and Session) from the object drop-down list in the Manage Subscriber Policies form.

3 Perform one of the following:

a Create a PPP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create PPP Policy. The PPP Policy - Global Policy (Create) form opens.

b Modify a PPP policy.

i Configure the filter criteria and click on the Search button. A list of PPP policies appears.

ii Select a PPP policy and click on the Properties button. The PPP Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- PPP MTU
- LCP Keep-Alive Interval (seconds)
- LCP Keep-Alive Hold Up Multiplier
- Disable AC Cookies
- PADO Delay (100’s of milliseconds)
- Maximum Sessions Per MAC
- Enable Reply On PADT
- Authentication Type
- Minimum CHAP Challenge Length
- Maximum CHAP Challenge Length
- Initial Delay
- IPCP Subnet Negotiation
- PPP MTU Force Greater Than 1492
- Unique Session ID per SAP
- Reject Disabled NCP
- PADO AC Name

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The PPP Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 46-1 for more information about distributing a policy.

7 Click on the Options tab. A list of options appears.

8 Perform one of the following:

a To add an option, go to step 12.

b To edit an existing option, go to step 9.

9 Choose an option from the list.

10 Click on the Properties button. The PPP Option (Edit) form opens.

11 Go to step 13.

12 Click on the Create button. The PPP Option (Create) form opens.

13 Configure the parameters:

- Option Protocol
- Custom Option Number
- Option Type
- Option Value
- IP Address

14 Click on the OK button to close the PPP Option (Create) form. A dialog box appears.

15 Click on the OK button. The PPP Option (Create) form closes.

Procedure 68-5 To create or modify an MSAP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 In the Manage Residential Subscriber form, choose Global as the Policy scope and right-click on the Create button to open the contextual menu.

3 Perform one of the following:

a Create a MSAP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create MSAP Policy. The MSAP Policy - Global (Create) form opens.

b Modify a MSAP Policy.

i Configure the filter criteria and click on the Search button. A list of MSAP policies appears.

ii Select a PPP policy and click on the Properties button. The MSAP Policy (Edit) form opens.

4 Configure the parameters on the General tab:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Security tab button and configure the parameters.

   i In the DoS Protection Policy area, click on the Select button to open the Select NE DoS Protection form and choose a NE DoS Protection.

   ii If MAC Monitoring is required, select the MAC Monitoring check box.

6 Click on the Subscriber Management tab button and configure the parameters.

- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Default Subscriber Profile
- Default SLA Profile
- Default Subscriber Identification Policy
- Default Application Profile
- Profiled Traffic Only
- Non-Subscriber Traffic Identification
- Non-Subscriber Traffic Subscriber Profile
- Non-Subscriber Traffic SLA Profile
- Non-Subscriber Traffic Application Profile

7 Click on the ATM tab button.

8 Configure the ATM OAM Alarm Cell Handling and Periodic ATM OAM Loopback parameters.

9 Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

10 Select an ingress ATM policy from the list and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the MSAP Policy - Global (Create) form refreshes with the ingress ATM policy information displayed.

11 Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

12 Select an egress ATM policy from the list and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the MSAP Policy - Global (Create) form refreshes with the egress ATM policy information displayed.

13 Perform the following as required:

   a Click on the VPLS Configuration Only tab button and configure the following tabs within the VPLS Configuration Only tab.

      i Click on the General tab button and configure the parameters:

      - Split Horizon Group Name
      - Displayed Name
      - ARP Reply Agent
      - LAG link selection

ii Click on the DHCP tab button and configure the parameters:

- Lease Populate
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- Administrative State
- Emulated Server IP Address
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

iii Click on the IGMP Snooping tab button and configure the parameters:

- IGMP Import Policy
- Fast Leave
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Name
- Description
- Default Action
- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- MVR Source Interface

b If this policy is for an MSAP on an IES or VPRN, click on the IES VPRN Only Configuration tab button and configure the Anti-Spoofing parameter to be Source IP and MAC Addr.

14 Click on the VPLS Multicast CAC Constraints tab button and configure the parameters as follows:

Note 1 — Up to eight Multicast CAC Level entries can be created for an MSAP policy.

Note 2 — Up to eight Multicast CAC LAG entries can be created for an MSAP policy

Note 3 — The Bandwidth (kbps) range is 1 to 4 294 967 952 for an MSAP policy.

i Click on the Create button in the LAG Port Down tab and configure the following parameters:

- Number of Ports Down
- Level ID

ii Click on the Create button in the Level tab and configure the following parameters:

- Level ID
- Bandwidth (kbps)

15 Click on the Apply button.

16 Click on the OK button.

Procedure 68-6 To create or modify a host tracking policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose Host Tracking Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a host tracking policy.

i Click on the Create button. A drop down menu appears.

ii Choose Host Tracking Policy. The Host Tracking Policy, Global Policy (Create) form opens.

b Modify a host tracking policy.

i Configure the filter criteria and click on the Search button. A list of host tracking policies appears.

ii Select a host tracking policy and click on the Properties button. The Host Tracking Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Rate Modification
- Rate Modification Scheduler

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The Host Tracking Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 46-1 for more information about distributing a policy.

7 Close the Host Tracking Policy (Edit) form.

Procedure 68-7 To create or modify a category map policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Category Map Policy from the contextual menu. The Category Map Policy (Create) form appears with the General tab displayed.

4 Perform one of the following:

a Create a category map policy.

i Click on the Create button. A drop down menu appears.

ii Choose Category Map Policy. The Category Map Policy, Global Policy (Create) form opens.

b Modify a category map policy.

i Configure the filter criteria and click on the Search button. A list of category map policies appears.

ii Select a category map policy and click on the Properties button. The Category Map Policy (Edit) form opens.

5 Configure the parameters:

- Displayed Name
- Description
- Credit Type
- Credit Exhuast Threshold (%)
- Activity Threshold (kbps)

6 Click on the Category tab button.

7 Click on the Create button. The Category (Create) form opens with the general tab displayed.

8 Configure the parameters:

- Displayed Name
- Description
- Credit Type Override
- Rating Group
- Out Of Credit Action
- Default Credit Type
- Default Credit Time (seconds)
- Default Credit Volume
- Default Credit Volume Unit
- PIR (kbps)

The Rating Group parameter is only configurable when the Use Rating Group check box is enabled.

The PIR (kbps) parameter is configured to its maximum value when the MAX check box is enabled.

Note — A maximum of three categories can be created for each category map policy.

9 Click on the Queues tab button.

10 Select any or all of the Ingress and Egress Queues to be defined in the category.

11 Click on the Policers tab button.

12 Select any or all of the Ingress and Egress Policers to be defined in the category.

13 Click on the Credit Exhausting Service Levels tab button.

14 Perform one of the following:

a To define credit exhausting service levels for IP filter entries, go to step 15.

b To define credit exhausting service levels for IPv6 filter entries, go to step 21.

15 Click on the IP Filter Entries tab button.

16 Click on the Create button. The Exhausted IP Filter Entry (Create) form opens with the General tab displayed.

17 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

18 Click on the Filter Properties tab button.

19 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask
- Fragment
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option

20 Go to step 26.

21 Click on the IPv6 Filter Entries tab button.

22 Click on the Create button. The Exhausted IPv6 Filter Entry (Create) form opens.

23 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

24 Click on the Filter Properties tab button.

25 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask

26 Click on the OK button. A dialog box appears.

27 Click on the OK button. The Category (Create) for reappears with the filter entries information displayed.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The Category Map Policy (Create) form reappears with the category information displayed.

30 Click on the OK button. The Category Map Policy (Create) form closes.

Procedure 68-8 To create or modify a credit control policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Credit Control Policy from the contextual menu. The Credit Control Policy (Create) form opens with the General tab displayed.

4 Perform one of the following:

a Create a credit control policy.

i Click on the Create button. A drop down menu appears.

ii Choose Category Map Policy. The Credit Control Policy (Create) form opens.

b Modify a credit control policy.

i Configure the filter criteria and click on the Search button. A list of credit control policies appears.

ii Select a category map policy and click on the Properties button. The Credit Control Policy (Edit) form opens.

5 Configure the parameters:

- Displayed Name
- Description
- Credit Control Server
- Out Of Credit Action
- Error Handling Action

6 Click on the Select button in the Category Map panel. The Select Category Map form opens.

7 Select a category map policy from the list to be used with the credit control policy and click on the OK button. The Select Category Map form closes.

8 If you selected a value of Diameter for the Credit Control Server parameter, click on the Select button in the Diameter Policy panel. The Select Diameter Policy form opens.

9 Select a diameter policy from the list to be used to access the credit control server and click on the OK button. The Select Diameter Policy panel closes.

10 Click on the OK button. The Credit Control Policy (Create) form closes.

Procedure 68-9 To create or modify an IGMP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose IGMP Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create an IGMP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create IGMP Policy. The IGMP Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify an IGMP policy.

i Configure the filter criteria and click on the Search button. A list of IGMP policies appears.

ii Select an IGMP policy and click on the Properties button. The IGMP Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Import Policy
- Maximum Number of Groups
- Administrative Version
- Fast Leave
- Redirection Policy

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Configure the parameters in the multicast reporting panel:

- Administrative State
- Destination Name
- SAP ID
- Service ID
- PPPoE Session ID
- Host MAC

6 Click on the Apply button. The IGMP Policy (Edit) form refreshes with the policy configuration mode information.

7 Click on the Static Group/Source tab button. A list of multicast static group/static source address pairs appears.

8 Perform one of the following:

a Select an address pair from the list and click on the Properties button. The IGMP Policy Static (Edit) form appears. Go to step 9.

b Click on the Create button. The IGMP Policy Static (Create) form appears. Go to step 9.

9 Configure the parameters:

- Static Multicast Group
- Static Source

10 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 46-1 for more information about distributing a policy.

11 Close the IGMP Policy (Edit) form.

Procedure 68-10 To create or modify a BGP Peering policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose BGP Peering Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a BGP Peering policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create BGP Peering Policy. The BGP Peering Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify a BGP Peering policy.

i Configure the filter criteria and click on the Search button. A list of BGP Peering policies appears.

ii Select a BGP Peering policy and click on the Properties button. The BGP Peering Policy (Edit) form opens.

4 Configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Displayed Name
- Description
- Cluster ID
- Local Address
- BGP Keychain
- MED Source
- MED Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The BGP Peering Policy (Edit) form refreshes with the policy configuration mode information.

6 Click on the Behavior tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Hold Time (seconds)
- Prefix Limit

7 Click on the AS Properties tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Peer AS
- Min AS Origination (seconds)
- Disable 4Byte ASN
- AS Override
- Local AS
- Remove Private AS

8 Click on the Import Policies tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

9 Click on the Export Policies tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

10 Click on the Authentication tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- MD5 Authentication
- Authentication Key

11 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 46-1 for more information about distributing a policy.

12 Close the BGP Peering Policy (Edit) form.

Procedure 68-11 To create or modify a diameter policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Perform one of the following.

a Create a diameter policy.

i Click on the Create button and choose Diameter Policy from the drop-down menu. The Diameter Policy (Create) form appears with the General tab displayed.

ii Go to step 3.

b Modify a diameter policy.

Caution — Modifying an active diameter policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the diameter policy before you proceed.

i Choose Diameter Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of diameter policies appears.

iii Select a diameter policy and click on the Properties button. The Diameter Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

4 On the Connection Origin panel, configure the Virtual Router Type parameter.

If you specified VPRN Service as the Virtual Router Type, you must also configure the Service Name parameter on the VPRN Service panel. Click on the Select button and choose a VPRN service from the Select VPRN Service - Diameter Policy form.

5 Configure the timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)

6 Click on the DCAA Parameters tab button.

7 Configure the parameters:

- Failover Support
- Failure Handling
- Tx Timer (seconds)
- Service Context ID
- RADIUS Called-Station-ID
- Include RADIUS User
- Origin Subscription ID
- Subscription ID Type

8 Click on the Peers tab button.

9 Click on the Create button. The Diameter Peer - Diameter Policy (Create) form appears with the General tab displayed.

10 Configure the parameters:

- Displayed Name
- Description
- Administrative State
- Preference
- IP Address
- Port Number
- Protocol
- Destination Host
- Destination Realm

11 If you want to specify local override settings for any of the timer settings for the peer, deselect the Inherit Value check box and then specify a value for any of the following timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)

Note — When the Inherit Value check box is selected for a timer parameter on a peer object, the timer value is inherited from the parent diameter policy.

12 Click on the OK button on Diameter Peer - Diameter Policy (Create) form. The Diameter Policy (Create) form reappears with the new peer displayed on the Peers tab.

13 Click on the OK button in the Diameter Policy (Create) form. The Manage Residential Subscriber Policies form reappears with the new diameter policy displayed in the list.

14 Close the Manage Residential Subscriber Policies form.

Procedure 68-12 To create or modify a subscriber multicast CAC policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber multicast CAC policy.

i Click on the Create button and choose Create Subscriber Multicast CAC Policy from the drop-down menu. The Subscriber Multicast CAC Policy (Create) form opens.

ii Go to step 3.

b Modify a subscriber multicast CAC policy.

i Choose Subscriber Multicast CAC Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber multicast CAC policies appears.

iii Select a subscriber multicast CAC policy and click on the Properties button. The Subscriber Multicast CAC Policy (Edit) form opens.

3 Configure any applicable parameters:

- Displayed Name
- Description
- Administrative State
- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Subscriber Multicast CAC Policy (Create) form closes.

5 Close the Manage Subscriber Policies form.

Procedure 68-13 To create or modify an SLA profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create an SLA profile.

i Click on the Create button and choose Create SLA Profile from the drop-down menu. The SLA Profile (Create) form opens.

ii Go to step 3.

b Modify an SLA profile.

Caution — Modifying an active SLA profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the SLA profile before you proceed.

i Choose SLA Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of SLA profiles appears.

iii Select an SLA profile and click on the Properties button. The SLA Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Application
- Description
- Host Limit
- Remove oldest Subscriber Host

The Displayed Name parameter is configurable only during SLA profile creation.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Credit Control Policy panel. The Select Credit Control Policy form opens.

5 Select a credit control policy from the list and click on the OK button. The Select Credit Control Policy form closes.

Note — If you select a credit control policy, you will not be able to select a category map in step 13.

6 Click on the QoS tab button to choose QoS policies for the SLA profile.

7 Perform one of the following steps using the buttons in the Ingress Policy and Egress Policy panels.

a Assign a policy.

i Click on the appropriate Select button to choose an ingress or egress QoS policy. The ingress or egress Select Policy - SLA Profile form opens.

ii Select a policy and click on the OK button. The Select Policy - SLA Profile form closes, and the SLA Profile (Create) form refreshes with the chosen policy.

iii Configure the ingress queue parameters:

- Use Shared Queue
- Use Multipoint Shared Queue
- Report Rate Type
- Report Rate Scheduler

iv Configure the egress QoS marking parameters:

- Use Egress QoS Marking From SAP
- Scheduler Type
- Report Rate Type
- Report Rate Scheduler

b Remove a policy.

i Click on the Clear button in the Ingress Policy or Egress Policy panel to remove an ingress or egress QoS policy. The policy is removed from the list.

ii If you want to assign a policy to replace the removed policy, go to step 7a.

8 Click on the ACL tab button to assign ingress or egress IP filters to the SLA profile, if required.

i Click on the Select button in the Ingress IP Filter panel to choose an ingress IP filter from the Select Ingress IP Filter - SLA Profile form.

ii Click on the Select button in the Egress IP Filter panel to choose an egress IP filter from the Select Egress IP Filter - SLA Profile form.

iii Click on the Select button in the Ingress IPv6 Filter panel to choose an ingress IPv6 filter from the Select Ingress IPv6 Filter - SLA Profile form.

iv Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress filter from the Select Egress IPv6 Filter - SLA Profile form.

9 Click on the Supported Service Models tab button to indicate the intended service model for the SLA profile.

Note — The 5750 SSC requires the specification of a service model for interoperation with the 5620 SAM.

10 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Bridged)

11 Click on the Category Map tab button.

12 Click on the Select button in the Category Map panel. The Select Category Map form opens.

13 Select a category map from the list and click on the OK button. The Select Category Map form closes.

Note — If you selected a credit control policy in step 5, you will not be able to select a category map.

14 Click on the Create... button in the Categories panel. The Category (Create) form opens.

15 Click on the Select button in the Category Name panel. The Select Category Name form opens.

16 Select a category name from the list and click on the OK button. The Select Category Name form closes and the Category (Create) form reappears with the category name displayed.

17 Configure the Idle Timeout (seconds) parameter.

Note — The session will be disconnected if the value of the Activity Threshold (kbps) parameter is not met during the period specified by the Idle Timeout (seconds) parameter. See procedure 68-7 for more information about configuring the Activity Threshold (kbps) parameter.

18 Click on the OK button. A dialog box appears.

19 Click on the OK button.

20 Click on the Override Policy Items tab button to specify local overrides for queue parameters of the QoS policies assigned to the SLA profile, if required. The Access Ingress Policy tab is displayed.

21 Perform either of the following:

a Modify the access ingress queue parameters.

i Click on the Create button. The Access Ingress Queue Override (Create) form opens with the General tab displayed.

ii Go to step 22.

b Modify the access egress queue parameters.

i Click on the Access Egress Queues tab button.

ii Click on the Create button. The Access Egress Queue Override (Create) form opens with the General tab displayed.

22 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue Select form opens.

ii Select a policy queue and click on the OK button. The policy queue Select form closes, and the Queue Override (Create) form refreshes with the configured values for the policy queue.

23 Click on the Override tab button and configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override High Priority Reserved
- Override Port Average Overhead
- Default
- CIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (kb)
- High Priority Reserved
- Port Average Overhead (%)

The Override Port Average Overhead and Port Average Overhead (%) parameters are configured only for access egress queues.

24 Click on the OK button to close the Queue Override (Create) form. A dialog box appears.

25 Click on the OK button. The SLA Profile (Create) form refreshes with the queue override entry.

26 Specify local overrides for statistics and traffic flow rate parameters of the ingress or egress policers assigned to the SLA profile, if required.

27 Perform either of the following:

a Modify the access ingress policer parameters.

i Click on the Access Ingress Policers tab button.

ii Click on the Create button. The Ingress Policer Override (Create) form opens with the General tab displayed.

iii Go to step 28.

b Modify the access egress policer parameters.

i Click on the Access Egress Policer tab button.

ii Click on the Create button. The Egress Policer Override (Create) form opens with the General tab displayed.

28 Choose the policy policer that you want to override.

i Click on the Select button. The policy policer Select form opens.

ii Select a policy policer and click on the OK button. The policy policer Select form closes, and the Policer Override (Create) form refreshes with the configured values for the policy policer.

29 Click on the Override tab button and configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Default
- CIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (kb)
- Stats Mode
- Packet Byte Offset

30 Click on the OK button to close the Policer Override (Create) form. A dialog box appears.

31 Click on the OK button. The SLA Profile (Create) form refreshes with the policy policer override entry.

32 Click on the OK button. A dialog box appears.

33 Click on the Yes button. The SLA Profile (Create) form closes.

34 Close the Manage Subscriber Policies form.

Procedure 68-14 To create or modify a subscriber profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber profile.

i Click on the Create button and choose Create Subscriber Profile from the drop-down menu. The Subscriber Profile (Create) form opens.

ii Go to step 3.

b Modify a subscriber profile.

Caution — Modifying an active subscriber profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber profile before you proceed.

i Choose Subscriber Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber profiles appears.

iii Select a subscriber profile and click on the Properties button. The Subscriber Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

Note 1 — You can designate a subscriber profile as the default profile by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber profile creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

Note 3 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when a scheduler is not specified in the Egress Scheduler panel.

4 Click on the Select button in the Accounting Policy panel. The Select Accounting Policy ID - Subscriber Profile form opens.

5 Select an accounting policy and click on the OK button. The Select Accounting Policy ID - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the accounting policy information.

6 Click on the Select button in the ANCP Policy panel. The Select ANCP Policy - Subscriber Profile form opens.

7 Select an ANCP policy and click on the OK button. The Select ANCP Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the ANCP policy information.

8 Click on the Select button in the Host Tracking Policy panel. The Select Host Tracking Policy - Subscriber Profile form opens.

9 Select a host tracking policy and click on the OK button. The Select Host Tracking Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the host tracking policy information.

10 Click on the Select button in the NAT Policy panel. The Select NAT Policy - Subscriber Profile form opens.

11 Select a NAT policy and click on the OK button. The Select NAT Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the NAT policy information.

12 Click on the Select button in the IGMP Policy panel. The Select IGMP Policy - Subscriber Profile form opens.

13 Select an IGMP policy and click on the OK button. The Select IGMP Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the IGMP policy information.

14 Click on the Select button in the Subscriber Multicast CAC Policy panel. The Select Subscriber Multicast CAC Policy - Subscriber Profile form opens.

15 Select a subscriber multicast CAC policy and click on the OK button. The Select Subscriber Multicast CAC Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the subscriber multicast CAC policy information.

16 Click on the Scheduling tab button.

17 Configure the parameters:

- Assign Aggregate Rate Limit
- Egress Aggregate Rate Limit (kbps)
- Average Frame Size
- Encapsulation Offset
- Frame Base Accounting

Note — An additional parameter, Encapsulation Offset Mode, can be configured using OSSI.

18 Perform one of the following steps using the buttons in the Ingress Scheduler and Egress Scheduler panels.

> **Note —** You cannot specify an egress scheduler in a subscriber profile when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

a Assign a scheduler.

i Click on the appropriate Select button to choose an ingress or egress scheduler. The ingress or egress Select Scheduler - Subscriber Profile form opens.

ii Select a scheduler and click on the OK button. The Select Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the chosen scheduler.

b Remove a scheduler.

i Click on the appropriate Clear button to remove an ingress or egress scheduler. The scheduler is removed from the Subscriber Profile (Create) form.

ii If you want to assign a scheduler to replace the removed scheduler, go to step 18a.

19 Click on the RADIUS Accounting tab button to associate a RADIUS-based accounting policy with the subscriber profile or to remove a RADIUS-based accounting policy from the subscriber profile.

20 Perform one of the following steps.

a Assign a RADIUS accounting policy by performing the following steps.

i Click on the Select button in the RADIUS Accounting Information panel. The Select RADIUS Accounting Information - Subscriber Profile form opens.

ii Configure the filter criteria.

iii Click on the Search button. A list of RADIUS accounting policies appears.

iv Select a policy from the list and click on the OK button. The Select RADIUS Accounting Information - Subscriber Profile form closes and the Subscriber Profile (Create) form refreshes with the RADIUS accounting policy information.

b Remove a RADIUS accounting policy.

i Click on the Clear button to remove a RADIUS accounting policy. The policy is removed from the Subscriber Profile (Create) form.

ii If you want to assign a policy to replace the removed policy, go to step 20a.

21 Perform one of the following steps to assign or remove a duplicate RADIUS accounting policy to generate duplicate accounting information for the subscriber profile.

a Assign a duplicate RADIUS accounting policy by performing the following steps.

i Click on the Select button in the Duplicate RADIUS Accounting Information panel. The Select Duplicate RADIUS Accounting Information - Subscriber Profile form opens.

ii Configure the filter criteria.

iii Click on the Search button. A list of RADIUS accounting policies appears.

iv Select a policy from the list and click on the OK button. The Select Duplicate RADIUS Accounting Information - Subscriber Profile form closes and the Subscriber Profile (Create) form refreshes with the duplicate RADIUS accounting policy information.

b Remove a duplicate RADIUS accounting policy.

i Click on the Clear button to remove a duplicate RADIUS accounting policy. The duplicate policy is removed from the Subscriber Profile (Create) form.

ii If you want to assign a duplicate policy to replace the removed duplicate policy, go to step 21a.

22 Click on the SLA Profiles tab button to associate an SLA profile with the subscriber profile or to remove an SLA profile from the subscriber profile. The General tab is displayed.

23 Configure the Use Direct Map as Default parameter.

24 Click on the Profiles tab button.

25 Perform one of the following.

a Assign an SLA profile.

i Click on the Create button. The SLAProfileEntry (Create) form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry (Create) form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

v Click on the OK button to close the SLAProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Profile (Create) form refreshes with the SLA profile entry.

b Remove an SLA profile.

i Select an SLA profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The SLA profile is removed from the list.

iii If you want to assign an SLA profile to replace the removed SLA profile, go to step 25 a.

26 Repeat step 25 for each additional SLA profile that you want to associate with the subscriber profile or remove from the subscriber profile.

27 Click on the HSMDA QoS tab button.

28 Perform one of the following.

a Assign an ingress policy.

i Click on the Select button in the Ingress Policy panel to choose an ingress policy. The Select Ingress Policy form opens.

ii Select a policy and click on the OK button. The Select Ingress Policy form closes, and the Subscriber Profile (Create) form refreshes with the chosen policy.

b Assign an egress policy.

i Configure the parameters:

- Assign Aggregate Rate Limit
- Egress Aggregate Rate Limit (kbps)

ii Click on the Select button in the Egress Policy panel to choose an egress policy. The Select Egress Policy form opens.

iii Select a policy and click on the OK button. The Select Egress Policy form closes, and the Subscriber Profile (Create) form refreshes with the chosen policy.

29 Configure the Packet Byte Offset (bytes) parameter in the Egress Policy Override panel, if required. You must enable the associated Override check box to be able to configure this parameter.

30 Click on the Select button in the Egress Policy Override panel to choose a WRR policy. The Select WRR Policy form opens.

31 Select a policy and click on the OK button. The Select WRR Policy form closes, and the Subscriber Profile (Create) form refreshes with the chosen policy.

32 Click on the Policer Control tab button to configure ingress and egress policer control policies, if required.

i On the Ingress Policer Control Policy panel, configure the Displayed Name parameter.

Click on the Select button next to the Displayed Name field and select a policy from the Select Policer Control Policy form.

ii You can configure local overrides on the selected ingress policer control policy on the Ingress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

iii On the Egress Policer Control Policy panel, configure the Displayed Name parameter.

Click on the Select button next to the Displayed Name field and select a policy from the Select Policer Control Policy form.

iv You can configure local overrides on the selected egress policer control policy on the Egress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

33 Click on the Override Policy Items tab button to modify the scheduler parameters for the subscriber profile, if required.

34 Perform one of the following.

a Modify the ingress scheduler parameters.

i Click on the Ingress Schedulers tab button.

ii Click on the Create button. The Ingress Scheduler Entry Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Ingress Scheduler Policy Entry form opens.

iv Select a scheduler policy and click on the OK button. The Select Ingress Scheduler Policy Entry form closes, and the Ingress Scheduler Entry Override (Create) form refreshes with the configured values for the scheduler policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

The CIR (kbps) parameter can only be configured when Summed CIR is set to false.

vii Click on the OK button to close the Ingress Scheduler Entry Override (Create) form.

b Modify the egress scheduler parameters.

i Click on the Egress Schedulers tab button.

ii Click on the Create button. The Egress Scheduler Entry Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Egress Scheduler Policy Entry form opens.

iv Select a policy and click on the OK button. The Select Egress Scheduler Policy Entry form closes, and the Egress Scheduler Entry Override (Create) form refreshes with the configured values for the policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

The CIR (kbps) parameter can only be configured when Summed CIR is set to false.

vii Click on the OK button to close the Egress Scheduler Entry Override (Create) form.

c Modify the access egress HSMDA queue parameters.

i Click on the Access Egress HSMDA Queues tab button.

ii Click on the Create button. The Access Egress HSMDA Queue Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Access Egress Policy Queue form opens.

iv Select a queue and click on the OK button. The Select Access Egress Policy Queue form closes, and the Access Egress HSMDA Queue Override (Create) form refreshes with the configured values for the policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- PIR (kbps)
- Maximum Burst Size (bytes)
- WRR Weight

If you enable the Override check box for any of these parameters, then the original value of the parameter that was configured for the Access Egress HSMDA Queue will appear in that parameter's value field. You can then configure the override value for that parameter.

You can only specify an override value for WRR Weight for queues 1, 2, or 3.

vii Click on the Select button. The Select HSMDA Slope Policy form opens.

viii Select a policy and click on the OK button. The Select HSMDA Slope Policy form closes, and the Access Egress HSMDA Queue Override (Create) form refreshes with the selected HSMDA Slope policy name displayed.

ix Click on the OK button to close the Access Egress HSMDA Queue Override (Create) form.

d Click on the Ingress Policer Level tab button to configure ingress policer priority level overrides, if required. An ingress policer control policy must be configured on the subscriber profile before these steps can be completed.

i Click on the Create button. The Ingress Policer Level Override Create form appears. The configured policer control policy appears in the Displayed Name field.

ii On the Policer Level panel, click on the Select button. The Select Policer Level form appears.

iii Select a policer level from the list and click OK. The Select Policer Level form closes and the selected level appears in the Level field on the Policer Level panel. The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.

iv To override the maximum cumulative buffer space value for the policer level, click on the Override tab button.

v On the Overridden Policer Level panel, enable the Override check box.

- **vi** Either enable the Max check box or configure the Cumulative MBS Contribution parameter.
- **vii** Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vii.

e Click on the Egress Policer Level tab button to configure egress policer priority level overrides, if required. An egress policer control policy must be configured on the subscriber profile before these steps can be completed.

- **i** Click on the Create button. The Egress Policer Level Override Create form appears. The configured policer control policy appears in the Displayed Name field.
- **ii** On the Policer Level panel, click on the Select button. The Select Policer Level form appears.
- **iii** Select a policer level from the list and click OK. The Select Policer Level form closes and the selected level appears in the Level field on the Policer Level panel. The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.
- **iv** To override the maximum cumulative buffer space value for the policer level, click on the Override tab button.
- **v** On the Overridden Policer Level panel, enable the Override check box.
- **vi** Either enable the Max check box or configure the Cumulative MBS Contribution parameter.
- **vii** Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vii.

35 Click on the OK button. The Subscriber Profile (Create) form refreshes with the scheduler override entry.

36 Click on the OK button to close the Subscriber Profile (Create) form. A dialog box appears.

37 Click on the Yes button. The Subscriber Profile (Create) form closes.

38 Close the Manage Subscriber Policies form.

Procedure 68-15 To manage residential subscriber management components on a SAP

Perform this procedure to manage the subscriber configuration on one or more SAPs. You can configure the subscriber-related SAP parameters and assign one or more of the following residential subscriber management components:

- subscriber identification policy
- default subscriber identification string
- default subscriber profile
- default SLA profile
- non-subscriber traffic subscriber profile
- non-subscriber traffic SLA profile

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to manage the SAPs; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

Note 1 — You can configure subscriber management on multiple SAPs at once from any list of SAP search results that the 5620 SAM generates. For simplicity, the procedure uses the term SAP to mean one or more SAPs, and focuses only on SAPs that belong to the same service site.

Note 2 — The 5620 SAM commits changes to a SAP configuration only when subscriber management is enabled on all SAPs that you are configuring.

7 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

8 Click on the Profiles tab button.

9 Perform one of the following steps for a component.

a Associate a component with the SAP.

i Click on the Select button beside the component in the Policies panel. The component Select Default form opens.

ii Select a component and click on the OK button. The component Select Default form closes, and the Policies panel refreshes with the component name.

b Remove a component, or replace an existing component with a new component.

Caution — Removing or replacing a residential subscriber management component on a SAP that is in use by subscriber hosts can be service-affecting to hosts that attempt to join the network. Ensure that removing the component does not affect the subscriber hosts before you proceed.

i Click on the Clear button beside the component in the Policies panel. The 5620 SAM removes the component from the Policies panel.

ii If you want to choose a component to replace the removed component, go to step 9 a.

10 Click on the OK button. The SAP configuration form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The service configuration form closes.

13 Close the Manage Services form.

Procedure 68-16 To enable or disable residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to enable or disable residential subscriber management on a SAP; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

7 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

8 Click on the Profiles tab button.

9 Configure the Admin Status parameter by performing one of the following.

   a Set the parameter to Enabled to enable residential subscriber management on the SAP.

   b Set the parameter to Disabled to disable residential subscriber management on the SAP.

10 Click on the OK button. The SAP configuration form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The service configuration form closes.

13 Close the Manage Services form.

Procedure 68-17 To create a static host for residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to create a static host for residential subscriber management on a SAP; expand the entries for that site.

5 Navigate to the SAPs that support subscriber management. Perform one of the following, depending on the type of service that you are configuring:

   a For an IES, the path is IES→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

   b For a VPLS, the path is VPLS→Site→Access Interfaces→*SAP*.

   c For a VPRN service, the path is VPRN→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab button. The General tab is displayed.

8 Configure the Anti-Spoofing parameter.

Note — You must set the Anti-Spoofing parameter to IP-address matching or to IP- and MAC-address matching before you can enable subscriber management for the static hosts on a SAP.

9 Click on the Static Hosts tab button.

10 Click on the Create button. The Access Interface Anti-Spoofing Static Host (Create) form opens with the General tab displayed.

11 Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

Note — To enable residential subscriber management for a static host, you must specify values for the IP Address and Subscriber Identification parameters.

12 Configure the Administrative State parameter.

13 Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with a list of available subscriber profiles.

Note — To enable residential subscriber management for a static host, you must specify a subscriber profile.

14 Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

15 Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with a list of available SLA profiles.

Note — To enable residential subscriber management for a static host, you must specify an SLA profile.

16 Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

17 Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with a list of local application profiles.

18 Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

19 Click on the OK button.

Note — The Administrative State parameter must be set to Up, to enable validation of Subscriber Identification, Subscriber Profile, and Application Profile.

Partially configured Static Hosts can be configured if the Administrative State parameter is set to Down.

20 Click on the Managed Routes tab button.

21 Click on the Create button.

22 The Access Interface Anti-Spoofing Static Host Managed Route Display (Create)form opens.

23 Configure the parameters:

- IP Address
- Prefix Length

24 Click on the OK button. A dialog box appears.

25 Click on the OK button.The Access Interface Anti-Spoofing Static Host Managed Route Display (Create) form closes.

Note — The creation of 16 managed routes is supported for each static host on IES and VPRN SAPs on the 7750 SR, 7450 ESS, and 7710 SR, Release 6.1 or later.

26 Click on the Apply button if you want to create an additional static host entry. A dialog box appears. Otherwise go to step 28.

27 Repeat steps 11 to 25 for each additional static host entry that you want to create.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The Access Interface Anti-Spoofing Static Host (Create) form closes, and the SAP configuration form refreshes with the new static host entries.

30 Click on the OK button. The SAP configuration form closes.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The service configuration form closes.

33 Close the Manage Services form.

Procedure 68-18 To configure a MEP on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to configure a MEP on a SAP; expand the entries for that site.

5 Perform one of the following steps.

- **a** To create a MEP on an Access Interface SAP, on the navigation tree, click on the site where you want to create the MEP; expand the entries for that site. Go to step 6

- **b** To create a Down MEP on a Subscriber Group Interface SAP, on the navigation tree, click on the site where you want to create the Down MEP; expand the entries for that site. Go to step 7.

Note 1 — MEPs can be configured on an Access Interface SAP for VPLS, VPRN, IES, and VLL Epipe services.

Note 2 — Down MEPs can be configured on a Subscriber Group Interface SAP for VPRN and IES.

6 Click on the Access Interfaces icon to display the site SAPs. Go to step 8.

7 Click on the Group Interfaces icon to display the site SAPs.

8 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

9 Click on the MEP tab button.

10 Click on the Create button. The MEP (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages Enabled
- Control MEP
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

The Control MEP parameter is only displayed if the Interface Type parameter is set to Ethernet Tunnel Path Endpoint.

Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab button.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The MEP (Create) form closes.

18 Close the Manage Services form.

Procedure 68-19 To list and manage subscriber management SAPs

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select one of the available SAP types from the object drop-down list:

- IES Service Access Point (ies)
- L2 Access Interface (mvpls)
- L2 Access Interface (vpls)
- VPRN Service Access Point (vprn)

3 Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs for the selected service type appears.

5 To view or manage the information for a particular SAP, select the entry from the list and click on the Properties button. The SAP Properties form opens on the General tab. You can view SAP information or make changes to a variety of parameters on the various tabs of the form.

6 Click on the OK button to implement any changes you have made.

7 Close the Properties form.

8 Close the Manage Residential Subscribers form.

Procedure 68-20 To create a Capture SAP

Use this procedure to create a Capture SAP, which enables the creation of an MSAP. A Capture SAP must be the default on a port.

Note 1 — A Capture SAP is not intended to carry traffic. The only purpose of the Capture SAP is to trigger the creation of an MSAP.

Note 2 — The MSAPs that are subsequently created will be on the same port as the Capture SAP.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the Capture SAP; expand the entries for that site.

5 Right-click on Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters as required for the service.

- SAP Sub Type, choose Capture from the SAP Sub Type drop-down menu.

Note — When you choose Capture as the SAP Sub Type, the displayed form changes to allow configuration of the Capture SAP.

- Description
- Administrative State

7 Click on the Port tab button.

8 Click on the Select button beside the Terminating Port Displayed parameter. The Select Terminating Port form appears.

9 Choose a terminating port from the list in the Select Terminating Port form.

10 Click on the DHCP tab button and add a Subscriber Authentication policy.

i Click on the Select button in the Subscriber Authentication Policy area. The Select Subscriber Authentication Policy - L2 access I/F window appears.

ii Filter the list to the Subscriber Authentication policy that you need.

iii Choose the required Subscriber Authentication policy.

11 Click on the Capture Access Interface tab button.

12 Perform one of the following to configure the Trigger Packet type:

a Select the check box beside one or two of the parameters that you want used to trigger RADIUS authentication. The parameters are:

- DHCP Trigger Packet
- PPPoE Trigger Packet
- ARP Trigger Packet
- PPP Trigger Packet

b Select the check box beside each of the parameters displayed to trigger RADIUS authentication when any or all of the trigger packets are received.

13 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name. The Select MSAP Policy - Capture L2 Access Interface form opens.

14 Configure the filter criteria. A list of available MSAP policies appears.

15 Choose an MSAP policy and click on the OK button. The Select MSAP Policy - Capture L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form appears with the MSAP policy name displayed.

16 Configure the parameters:

- MSAP Service ID
- MSAP Group Interface Name

17 Click on the Select button in the PPPoE Policy panel. The Select PPPoE Policy form opens.

18 Select a PPPoE policy from the list and click on the OK button. The Select PPPoE Policy form closes.

19 Click on the Select button in the PPP Policy panel. The Select PPP Policy form opens.

20 Select a PPP policy from the list and click on the OK button. The Select PPP Policy form closes.

21 Click on the Select button in the PPPoE Local User DB panel. The Select PPPoE Local User DB form opens.

22 Select a PPPoE Local User DB from the list and click on the OK button. The Select PPPoE Local User DB form closes.

23 Click on the Select button in the PPP Local User DB panel. The Select PPP Local User DB form opens.

24 Select a PPP Local User DB from the list and click on the OK button. The Select PPP Local User DB form closes.

25 Click on the Select button in the Redundancy panel. The Select SRRP Instance form opens.

26 Select an SRRP Instance from the list and click on the OK button. The Select SRRP Instance form closes.

27 Click on the ATM tab button.

28 Configure the AAL5 Encapsulation parameter.

29 Click on the VC Ranges tab button.

30 Click on the Create button. The ATM Configuration (Create) form opens.

31 Configure the parameters:

- VC Range Index
- VPI Range Start
- VPI Range End
- VCI Range Start
- VCI Range End

32 Click on the OK button. A dialog box appears.

33 Click on the OK button. The ATM Configuration (Create) form closes.

34 Click on the Apply button.

35 Click on the OK button.

Procedure 68-21 To list MSAPs and view MSAP properties

Use this procedure to list MSAPs and view MSAP properties.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Access Interface (Service Management) from the list.

3 Perform one of the following to display the MSAPs associated with each service:

a For VPLS MSAPs:

i Click on the L2 Access Interface (Service Management).

ii Click on the Abstract L2 Access Interface (VPLS) icon.

iii Click on the L2 Access Interface (VPLS) icon.

iv Click on the VPLS L2 Access Interface icon.

v Choose VPLS MSAP and click on the Search button.

b For IES MSAPs:

i Click on the Service Access Point icon (Service Management).

ii Click on the IES Service Access Point (IES) icon.

iii Choose IES MSAP and click on the Search button.

c For VPRN MSAPs:

i Click on the Service Access Point icon (Service Management).

ii Click on the VPRN Service Access Point (VPRN) icon.

iii Choose VPRN MSAP and click on the Search button.

4 Choose an MSAP from the list and click on the MSAP Properties tab button to view the MSAP properties.

Procedure 68-22 To view an MSAP event log, modify the global MSAP log policy, and purge MSAP log records

Use this procedure to view the event log for an MSAP, modify the global MSAP log policy, or purge the log records in an MSAP event log.

1 Perform Procedure 68-21 to list the MSAPs and choose the appropriate MSAP.

2 Click on the Events tab button to display the MSAP event log.

3 If you need to view an event log record, choose a record from the event log and click on the Properties button. The Statistics Record - MSAP Event Log form opens and displays the MSAP record properties.

4 Close the Statistics Record - MSAP Event Log form.

5 If you need to modify the global MSAP event log policy click on the Log Policy button. The Log Policy - Ressubscr. MSap Event Log form opens.

Note — The global MSAP log policy affects all MSAP event logs.

6 Configure the parameters:

- Retention Time (hours)
- Administrative State

7 Click on the Apply button to save the changes.

8 Close the Log Policy - Ressubscr. MSap Event Log form.

9 If you need to purge the MSAP event log records, click on the Purge Log Records button.

10 Click on the OK or Cancel button to close the Log Policy - Ressubscr. MSap Event Log form.

11 Click on the Close button to close the Statistics Record - MSAP Event Log form.

Procedure 68-23 To modify and re-evaluate an MSAP policy on an MSAP

Use this procedure to re-apply an MSAP policy on an existing MSAP. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form appears.

2 Configure the filter criteria. See Procedure 68-21 for more information about configuring the filter to list MSAPs. A list of MSAPs for the service appears.

3 Choose an MSAP and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the MSAP Properties tab button.

5 Click on the Properties button in the Creation MSAP Policy area and enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the MSAP Properties tab button.

7 Choose the Do Action option from the Creation MSAP Policy Re-evaluation parameter to apply the policies new parameter values. When you choose Not Applicable, the new parameter values in the policy are not applied but remain in the policy until you choose the Do Action option.

8 Click on the Apply button.

9 Click on the OK button.

Procedure 68-24 To modify an MSAP policy and re-evaluate the MSAPs

Use this procedure to re-apply an MSAP policy on existing MSAPs. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form appears.

2 Choose the policy scope as required. The policy scope can be Global or Local.

3 Configure the filter criteria to list MSAPs for the service. Choose MSAP Policy (MSAP Policy) and click on the Search button. A list of MSAP policies appears in the form.

4 Choose an MSAP policy and click on the Properties button. The MSAP Policy (Edit) form appears with the General tab displayed.

5 Enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the Reevaluate MSAPs button. The MSAPs are re-evaluated with the changed MSAP policy.

7 Click on the Apply button.

8 Click on the OK button.

Procedure 68-25 To delete an MSAP

Use this procedure to delete any MSAP that is an inactive state. Verify that the MSAP is in an inactive state. The 5620 SAM prevents attempts to delete an MSAP that is in an active state.

1. Perform Procedure 68-21 to list the MSAPs and choose the appropriate MSAP to delete.
2. Click on the Delete button. A dialog box appears.
3. Click on the Yes button in the dialog box. The MSAP is deleted.

Procedure 68-26 To delete an MSAP policy

Use this procedure to delete any MSAP policy on an MSAP that is an inactive state. Ensure that the MSAP is inactive and that the policy is not associated with other MSAPs that may be used at a later date. Do not attempt to delete MSAP policies on MSAPs that are in an active state.

1. Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.
2. In the Manage Residential Subscriber form, choose the Policy scope.
3. Choose MSAP Policy (MSAP Policy) from the list.
4. Click on the Search button in the Manage Residential Subscriber form. The MSAP policies are listed in the MSAP Policy list window.
5. Choose one or more MSAP policies that you need to delete.
6. Click on the Delete button. A dialog box appears.
7. Click on the Yes button in the dialog box. The MSAP policy is deleted.

Procedure 68-27 To configure DHCP event monitoring for a SAP

1. Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.
2. Select one of the available SAP types from the object drop-down list:
   - IES Service Access Point (ies)
   - L2 Access Interface (mvpls)
   - L2 Access Interface (vpls)
   - VPRN Service Access Point (vprn)
3. Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs appears.

5 To configure DHCP monitoring for a particular SAP, select the entry from the list and click on the Create Monitored SAP button. The Monitored Access Interface (Create) form opens with the General tab displayed.

Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

6 Configure the parameters:

- Monitoring Period
- Units

7 Click on the OK button to close the Monitored Access Interface (Create) form.

Note — You must complete Procedure 68-28 to enable and schedule SAP monitoring.

8 Close the Manage Residential Subscribers form.

Procedure 68-28 To monitor DHCP events for a SAP

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Access Interface from the object drop-down list.

3 Configure the filter criteria at the top-right panel of the form, if required.

4 Click on the Search button. A list of Monitored SAPs appears.

5 To initiate or view DHCP monitoring for a particular SAP, select the entry from the list and click on the Properties button. The Monitored Access Interface (Edit) form opens on the General tab.

6 You can perform one or more of the following on this form:

a To start monitoring the chosen SAP, click on the Start Monitor button.

b To stop monitoring the chosen SAP, click on the Stop Monitor button.

c To remove monitoring of the chosen SAP, click on the Delete button.

d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

7 To view DHCP events for the chosen SAP, click on the Events tab. The DHCP Events list is displayed.

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Access Interface form.

10 Close the Manage Residential Subscribers form.

Procedure 68-29 To configure DHCP lease management for a subscriber host

DHCP is used to assign IP addresses to hosts or workstations on the network. This function is usually performed by a DHCP server. Essentially, it "leases" out addresses for specific times to the various hosts. If a host does not use a specific address for a set period of time, that IP address can then be assigned to another machine by the DHCP server.

In order to allow the DHCP client to lease out address for specific times, the 5620 SAM allows an operator to force the DHCP client to change its state by sending a renewal command. Upon receipt of the renewal command from the 5620 SAM, the DHCP client changes to the renewal state and then negotiates with the DHCP server for lease times.

Conversely, an operator can also terminate (clear) a lease for a particular host from within the Residential Subscriber Host form of 5620 SAM.

Note — The DHCP lease renewal and termination are supported only on dynamic hosts, not on static hosts or subscriber hosts.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select Residential Subscriber Host from the object drop-down list.

3 Click on the Search Subscriber Host Information from Last Resynch radio button.

4 Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

5 Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

6 Configure the Service ID parameter.

7 Click on the Select button beside Port to specify a port. The Select Port form opens.

8 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

9 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

Note — The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

10 Click on the Search button. A list of subscriber hosts is displayed.

11 Select one or more entries in the list.

Note — You can renew a lease for multiple entries. However, you can perform a lease termination for only one host at a time.

12 Perform one of the following steps.

a To renew the lease, click on the Force Renew button.

b To terminate the lease, click on the Clear Lease State button.

13 A dialog box appears. Click on the Yes button. The action is completed.

14 Close the Manage Residential Subscribers form.

Procedure 68-30 To configure DHCP event monitoring for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Hosts from the object drop-down list.

3 Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

4 Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

5 Configure the Service ID parameter.

6 Click on the Select button beside Port to specify a port. The Select Port form opens.

7 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

8 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

Note — The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

9 Click on the Search button. A list of subscriber hosts appears.

10 To configure DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Create Monitored Host button. The Monitored Subscriber Host form opens.

Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

11 Configure the parameters:

- Monitoring Period
- Units
- Polling Interval

12 Click on the OK button to close the Monitored Subscriber Host form.

Note — You must complete Procedure 68-31 to enable and schedule subscriber host monitoring.

13 Close the Manage Residential Subscribers form.

Procedure 68-31 To monitor DHCP events for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Subscriber Host from the object drop-down list.

3 Configure the filter criteria at the top right panel of the form, if required.

4 Click on the Search button. A list of monitored subscriber hosts appears.

5 To initiate or view DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Properties button. The Monitored Subscriber Host (Edit) form opens with the General tab displayed.

6 You can perform one or more of the following on this form:

a To start monitoring the chosen subscriber host, click on the Start Monitor button.

b To stop monitoring the chosen subscriber host, click on the Stop Monitor button.

c To remove monitoring of the chosen subscriber host, click on the Delete button.

d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

e To change the Polling Interval, click on the Stop Monitor button and then select the desired value from the drop-down menu.

7 To view DHCP events for the chosen subscriber host, click on the Events tab. The DHCP Events list is displayed.

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Subscriber Interface form.

10 Close the Manage Residential Subscribers form.

Procedure 68-32 To configure a local user database to authenticate DHCP clients

A local user database is used by a local DHCP server to authenticate DHCP clients that request IP addresses. A group interface uses the local user database to authenticate a PPPoE clients that request IP addresses.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Local User Database (localuserdb) from the object drop-down list.

3 Perform one of the following steps:

a To create a local user database, click on the Create Local User Database button. A Local User Database (Create) window opens with the General tab displayed. Go to step 6.

b To modify an existing database, click on the Search button. A list of existing databases is displayed. Go to step 4.

4 Choose a database from the list.

5 Click on the Properties button. The Local User Database (Edit) form opens with the General tab displayed.

6 Click on the Select button in the Site panel to specify an NE. The Select a Local User Database Capable Network Element form opens.

7 Select an NE in the list and click on the OK button. The Select a Local User Database Capable Network Element form closes and the NE system address is displayed on the Local User Database (Create) form.

8 Configure the parameters.

- Displayed Name
- Description
- Administrative State

9 Click on the DHCP tab button. The DHCP Match List form is displayed.

10 Configure the parameters.

- Match Type DHCP 1
- Match Type DHCP 2
- Match Type DHCP 3
- Match Type DHCP 4

11 Click on the Masks tab button.

12 Click on the Create button. The Local User Database Dhcp Mask form is displayed.

13 Configure the parameters:

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length

14 Click on the Hosts tab button.

15 Click on the Create button. The Local User DB DHCP Host (Create) form opens with the General tab displayed.

16 Configure the parameters:

- Host Name
- Administrative State
- Domain Name
- Server Address

17 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - Local User DB DHCP Host form opens.

18 Configure the filter criteria. A list of available policies appears.

19 Select a policy and click on the OK button. The Select Subscriber Authentication Policy - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form reappears with the policy name information displayed.

20 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name. The MSAP Policy - Local User DB DHCP Host form opens.

Note — You can also enter text in the fields next to the MSAP Policy Name, MSAP Service ID, and MSAP Group Interface Name parameters.

21 Configure the filter criteria. A list of available MSAP policies appears.

22 Select an MSAP policy and click on the OK button. The MSAP Policy - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the MSAP policy name displayed.

23 Click on the Select button in the MSAP Defaults panel to choose an MSAP Service ID. The Service - Local User DB DHCP Host form opens with a list of services displayed.

24 Select a service and click on the OK button. The Service - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the service information displayed.

25 Click on the Select button in the MSAP Defaults panel to choose an MSAP Group Interface Name. The Group Interface - Local User DB DHCP Host form opens with a list of group interfaces displayed.

26 Select a group interface and click on the OK button. The Group Interface - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the group interface information displayed.

27 Click on the Address tab button. Configure only one of the following parameters.

- IP Address
- Use GI Address
- IP Address Pool Name
- Use Client Pool

28 Configure the IPv6 addressing parameters, if required:

- IPv6 Address
- IPv6 Prefix
- IPv6 Prefix Length

29 Click on the Host Identification tab button. Configure 4 of the following parameters.

- Circuit ID Format
- Circuit ID
- MAC Address
- Option 60
- Remote ID Format
- Remote ID
- SAP ID
- Service ID
- DHCP String
- System ID

30 Click on the Identification Strings tab button. Configure the Option Number parameter. The window is refreshed with additional parameters.

31 Configure the parameters.

- ANCP String
- Application Profile
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID

32 Click on the Options tab button. The Options form is displayed.

33 Click on the Create button. A Local User Database DHCP Option form opens.

34 Configure the Option Depending on the Option Value different parameters must be configured for each option.

35 Perform one of the following steps:

a Configure Custom Option, Subnet Mask, Default Routers, DNS Name Servers, and Netbios Name Server options. Go to step 36.

- Number
- Type
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

b Configure Lease Time, Lease Renew Time and Lease Rebind Time options. Go to step 36.

- Days
- Hours
- Minutes
- Seconds

c To configure the Domain Name option, configure the Option Value Go to step 36.

d To configure Netbios Node Type option, configure the Netbios Node Type parameter. Go to step 36.

36 Click on the OK button. A confirmation dialog box appears.

37 Click on the OK button. The Local User Database DHCP Option window closes and the Local User DB DHCP Host (Create) window is refreshed with the new options.

38 Click on the OK button.

39 Click on the PPPoE tab button. The PPPoE Match List form opens.

40 Configure the parameters.

- Match Type PPPoE 1
- Match Type PPPoE 2
- Match Type PPPoE 3

41 Click on the Masks tab button.

42 Click on the Create button. The Local User Database PPPoE Mask form opens.

43 Configure the parameters.

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length

Note — You must configure the Mask Type parameter before you configure the remaining parameters on the Local User Database PPPoE Mask form.

44 Click on the Hosts tab button.

45 Click on the Create button. The Local User DB PPPoE Host (Create) form opens with the General tab displayed.

46 Configure the parameters.

- Host Name
- Administrative State
- Retail Service ID
- PADO Delay (100’s of milliseconds)

47 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - Local User DB PPPoE Host form opens.

48 Configure the filter criteria. A list of available policies appears.

49 Choose a policy and click on the OK button. The Select Subscriber Authentication Policy - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form reappears with the policy name displayed.

50 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name The MSAP Policy - Local User DB PPPoE Host form opens.

Note — You can also enter text in the fields next to the MSAP Policy Name, MSAP Service ID, and MSAP Group Interface Name parameters.

51 Configure the filter criteria. A list of available MSAP policies appears.

52 Select an MSAP policy and click on the OK button. The MSAP Policy - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the MSAP policy name displayed.

53 Click on the Select button in the MSAP Defaults panel to choose an MSAP Service ID. The Service - Local User DB PPPoE Host form opens with a list of services displayed.

54 Select a service and click on the OK button. The Service - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the service information displayed.

55 Click on the Select button in the MSAP Defaults panel to choose an MSAP Group Interface Name. The Group Interface - Local User DB PPPoE Host form opens with a list of group interfaces displayed.

56 Select a group interface and click on the OK button. The Group Interface - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the group interface information displayed.

57 Click on the Address tab button. Configure one of the following parameters:

Note — If more than one IP address parameter is configured, the 5620 SAM displays an error message.

- IP Address
- IP Address Prefix Length
- Use GI Address
- IP Address Pool Name
- Use Client Pool

58 Click on the Host Identification tab button. Configure only 3 of the following parameters:

Note 1 — Circuit ID Format and Circuit ID are considered one parameter.

Note 2 — User Name Format and User Name are considered one parameter.

- Prefix String
- Circuit ID
- MAC Address
- Remote ID Format
- Remote ID
- Service Name
- User Name Format
- User Name

59 Configure the following parameters:

- Password Type
- Password

60 Click on the Identification Strings tab button. Configure the Option Number parameter. The window is refreshed with additional parameters.

61 Configure the parameters.

- ANCP String
- Application Profile
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID

62 Click on the L2TP tab button. A list of available tunnel groups appears.

Note — L2TP configuration is required on an NE that has the LAC role if RADIUS authentication is not used for PPPoE clients.

63 Click on the Select button next to the Group Name parameter to choose a tunnel group name. The Select Tunnel Group Name - Local User DB PPPoE Host form opens.

64 Configure the filter criteria and click on the Search button. A list of available tunnels is displayed.

65 Choose a tunnel group and click on the OK button. The Select Tunnel Group Name - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form reappears with the Group Name displayed.

66 Click on the Options tab button.

67 Click on the Create button. A Local User DB PPPoE Option form opens.

68 Configure the parameters:

- Option
- Number
- Type
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Option Value parameter is configurable when the Type parameter is set to ASCII string or Hex String.

69 Click on the OK button. A confirmation dialog box opens.

70 Click on the OK button. The Local User DB PPPoE Host (Create) form is refreshed with the new options.

71 Close the Local User DB PPPoE Host (Create) form.

72 Click on the following tab buttons to view information:

- Local DHCP Servers
- Group Interfaces
- Subscriber Authentication Policies
- Faults

73 Close the Local User Database (Edit) form.

Procedure 68-33 To configure NE SHCV event handling

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose Network Element SHCV from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NEs appears.

5 Select an NE and click on the Properties button. The Network Element SHCV (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Trap Dropped Raises Alarm
- Rate Exceeded Raises Alarm
- Maximum Sessions Per MAC

7 Click on the OK button. The Network Element SHCV (Edit) form closes, and a dialog box appears.

8 Click on the Yes button.

9 Close the Subscriber Host Connectivity Verification form.

10 Close the Manage Residential Subscribers form.

Procedure 68-34 To create or modify a subscriber explicit map

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

- **a** Create a subscriber explicit map entry.
  - **i** Click on the Create button and choose Create Subscriber Explicit Map Entry from the drop-down menu. The Subscriber Explicit Map Entry (Create) form opens.
  - **ii** Go to step 3.
- **b** Modify a subscriber explicit map entry.

  Caution — Modifying an active subscriber explicit map entry is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber explicit map entry before you proceed.

  - **i** Choose Subscriber Explicit Map Entry from the object drop-down list.
  - **ii** Configure the filter criteria and click on the Search button. A list of subscriber explicit map entries appears.
  - **iii** Select a subscriber explicit map entry and click on the Properties button. The Subscriber Explicit Map Entry (Edit) form opens.

3 Configure the parameters:

- Subscriber Identification
- Description
- Subscriber ID Alias

The Subscriber Identification parameter is configurable only during subscriber explicit map creation.

4 Click on the Select button in the Subscriber Profile panel to associate a subscriber profile with the subscriber explicit map. The Select Subscriber Profile form opens.

5 Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the Subscriber Explicit Map Entry (Create) form refreshes with the subscriber profile.

6 Click on the Select button in the SLA Profile panel to associate an SLA profile with the subscriber explicit map. The Select SLA Profile form opens.

7 Select an SLA profile and click on the OK button. The Select SLA Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the SLA profile.

8 Click on the Select button in the Application Profile panel to associate an application profile with the subscriber explicit map. The Select Application Profile form opens.

9 Select an application profile and click on the OK button. The Select Application Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the application profile.

Note 1 — The global AA group policy must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 2 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

10 Click on the OK button to close the Subscriber Explicit Map Entry (Create) form.

Procedure 68-35 To retrieve PPPoA sessions

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Subscribers form opens.

2 Choose PPPoA Session (PPP Policy and Session) from the object drop-down list in the Manage Subscribers form.

3 Click on the Select button next to the Site ID parameter. The Select an ESM Capable Network Element form opens.

4 Select a network element from the list and click on the OK button. The Select an ESM Capable Network Element form closes.

5 Click on the Select button next to the Service ID parameter. The Select a Service Site form opens.

6 Select a service site from the list and click on the OK button. The Select a Service Site form closes.

7 Click on the Select button next to the Service Access Point parameter. The Select a Service Access Point form opens.

8 Select a service access point from the list and click on the OK button. The Select a Service Access Point form closes.

9 Click on the Search button. A list of applicable PPPoA sessions appears.

10 Select a PPPoA session from the list and click on the Properties button. The PPPoA Session form opens.

11 Review the PPPoA session information.

12 Close the PPPoA Session form.

13 Close the Manage Subscribers form.

Procedure 68-36 To configure a MEP on an SDP Binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to configure a MEP on an SDP Binding; expand the entries for that site.

Note — MEPs can be configured on a SDP Binding for VPLS, VPRN, and VLL Epipe services.

5 Click on the Spoke SDP Bindings icon to display the site Spoke SDP Bindings.

6 Select one or more Spoke SDP Bindings, right-click, and choose Properties. The Spoke SDP Bindings configuration form opens with the General tab displayed.

7 Click on the Meps tab button.

8 Click on the Create button. The MEP (Create) form opens.

9 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

10 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab button.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The MEP (Create) form closes.

18 Close the Manage Services form.

Procedure 68-37 To configure L2Aware static port forwarding on a residential subscriber instance

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

4 Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

5 Click on the NAT Static Port Forwarding tab button.

6 Click on the Create button. The NAT Static Port Forwarding Display (Create) form opens.

7 Configure the parameters:

- Inside IP Address
- Outside IP Address
- Inside Port
- Protocol
- Outside Port
- Lifetime (seconds)

Note — You cannot specify the same set of Inside Port and Protocol values in more than one static port mapping to an Inside IP Address.

You can specify the same Outside Port value in multiple mappings to an Inside IP Address.

8 Click on the OK button. The NAT Static Port Forwarding Port Display (Create) form closes, and the new entry is listed on the Residential Subscriber (Edit) form.

9 Perform the following steps to synchronize NAT static port forwards, if required.

i Choose a static port forward from the list and click on the Sync button. The NAT Static Port Forwarding Sync form opens.

ii Click on the Select button in the Targeted Router Instance panel. The Select Targeted Router Instance form opens.

iii Select a router instance from the list and click on the OK button. The Select Targeted Router Instance form closes and the NAT Static Port Forwarding Sync form reappears with the router instance information displayed.

iv Configure the Lifetime (seconds) parameter and click on the OK button. A dialog box appears.

v Click on the OK button.

10 Close the Residential Subscriber (Edit) form.

11 Close the Manage Residential Subscribers form.

Procedure 68-38 To resynchronize static port forwarding entries

Because of the potentially large number of static port forwarding entries, the entries are not resynchronized during a full NE resynchronization. Perform this procedure to manually resynchronize the entries, if required.

Note — The 5620 SAM static port forwarding entries are current and do not require resynchronization if the following conditions are true.

- The 5620 SAM is used to create, maintain, and delete each entry.
- Each entry has an infinite lifetime, so is truly static.

1 Right-click on an NE in the navigation tree and choose Resync→Customized Resync from the contextual menu. The Resync Sites step form opens with the Resync Options step displayed.

2 Select Choose MIB entries.

3 Click on the Next button. The Choose MIB Entries step is displayed.

4 Select tmnxNatFwdEntry in the list.

5 Click on the Next button. The Force Resync step is displayed.

6 Select the Ignore Timestamps parameter.

7 Click on the Finish button. The entries are refreshed.

Note — You can view the static port forwarding entries on the NAT Static Port Forwarding tab of the NAT Configuration form for the following:

- base or service routing instances
- residential subscriber instances

Procedure 68-39 To collect, view, and clear host tracking statistics and information

Use this procedure to perform one or more of the following:

- collect, view, and clear on-demand host tracking statistics and information for a residential subscriber instance
- collect, view, and clear on-demand host tracking statistics and information for a VPLS L2 access interface
- collect, view, and clear on-demand host tracking statistics and information for an IES service access point
- collect, view, and clear on-demand host tracking statistics and information for a VPRN service access point
- clear statistics and host tracking information for a VPLS, VPRN, or IES service site
- clear statistics and host tracking information for a residential subscriber host

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 To collect, view, and clear on-demand host tracking statistics and information for a residential subscriber instance.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Instance (Residential Subscriber) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

iv Choose a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

v Click on the Statistics tab button.

vi Choose Host Tracking Stats (Residential Subscriber) from the object drop-down list.

vii Click on the Collect button to collect the statistics.

viii Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

ix View the statistics information.

x Click on the Close button to close the statistics record form.

xi Repeat steps viii to x for each statistics record that you want to view.

xii Click on the Host Tracking Info tab button.

xiii Configure the filter criteria and click on the Search button. Host tracking data for the residential subscriber instance appears.

xiv Click on the Clear button. A dialog box appears.

xv If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xvi Click the Yes button. An information box appears.

xvii Click the OK button. The data is deleted from the NE.

xviii Click the Clear Status tab button to view a list of host tracking information clear results.

xix Choose a request and click on the Properties button to view information about the request, if required.

xx Close the Residential Subscriber Instance (Edit) form.

xxi Close the Manage Residential Subscribers form.

2 To collect, view, and clear on-demand host tracking statistics and information for a VPLS L2 access interface.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on an access interface. The VPLS L2 Access Interface (Edit) form opens.

vi Click on the Statistics tab button.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps ix to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab button.

xiv Click on the Host Tracking Info tab button.

xv Configure the filter criteria and click on the Search button. Host tracking data for the L2 access interface appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab button to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the VPLS L2 Access Interface (Edit) form.

xxiv Close the VPLS Service (Edit) form.

xxv Close the Manage Services form.

3 To collect, view, and clear on-demand host tracking statistics and information for an IES service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a service access point. The IES Service Access Point (Edit) form opens.

vi Click on the Statistics tab button.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the host tracking statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps ix to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab button.

xiv Click on the Host Tracking Info tab button.

xv Configure the filter criteria and click on the Search button. Host tracking data for the IES service access point appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab button to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the IES Service Access Point (Edit) form.

xxiv Close the IES Service (Edit) form.

xxv Close the Manage Services form.

4 To collect, view, and clear on-demand host tracking statistics and information for a VPRN service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a service access point. The VPRN Service Access Point (Edit) form opens.

vi Click on the Statistics tab button.

vii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

viii Click on the Collect button to collect the host tracking statistics.

ix Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

x View the statistics information.

xi Click on the Close button to close the statistics record form.

xii Repeat steps vi to xi for each statistics record that you want to view.

xiii Click on the Subscriber Management tab button.

xiv Click on the Host Tracking Info tab button.

xv Configure the filter criteria and click on the Search button. Host tracking data for the VPRN service access point appears.

xvi Click on the Clear button. A dialog box appears.

xvii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xviii Click the Yes button. An information box appears.

xix Click the OK button. The data is deleted from the NE.

xx Repeat steps xvi to xix for each host that you need to clear.

xxi Click the Clear Status tab button to view a list of host tracking information clear results.

xxii Choose a request and click on the Properties button to view information about the request, if required.

xxiii Close the VPRN Service Access Point (Edit) form.

xxiv Close the VPRN Service (Edit) form.

xxv Close the Manage Services form.

5 To clear on-demand host tracking statistics and information for a VPLS service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The VPLS Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab button.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab button to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the VPLS Site (Edit) form.

xiv Close the VPLS Service (Edit) form.

xv Close the Manage Services form.

6 To clear on-demand host tracking statistics and information for an IES service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The IES Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab button.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab button to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the IES Site (Edit) form.

xiv Close the IES Service (Edit) form.

xv Close the Manage Services form.

7 To clear on-demand host tracking statistics and information for a VPRN service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v On the navigation tree, click on a site. The VPRN Site (Edit) form opens with the General tab displayed.

vi Click on the IGMP Host Tracking tab button.

vii Click on the Clear button. A dialog box appears.

viii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

ix Click the Yes button. An information box appears.

x Click the OK button. The service site data is deleted from the NE.

xi Click the Clear Status tab button to view a list of site host tracking information clear results.

xii Choose a request and click on the Properties button to view information about the request, if required.

xiii Close the VPRN Site (Edit) form.

xiv Close the VPRN Service (Edit) form.

xv Close the Manage Services form.

8 To clear on-demand host tracking statistics and information for a residential subscriber host.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Host (Residential Subscriber) from the object drop-down list.

iii Select the Search Current Subscriber Host Information option.

iv Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

v Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

vi Configure the Service ID parameter.

vii Click on the Select button beside Port to specify a port. The Select Port form opens.

viii Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

ix Click the Search button. A list of hosts appears.

x Choose a host from the list and click the Clear Host Tracking button. A dialog box appears.

xi If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? check box.

xii Click the Yes button. An information box appears.

xiii Click the OK button. The residential subscriber host data is deleted from the NE.

xiv You can view a list of the residential host clear results by clicking on the Clear Status button on the residential subscriber instance form.

xv Repeat steps x to xiv for each host that you need to clear.

xvi Close the Manage Residential Subscribers form.

Procedure 68-40 To view subscriber host information

ESM Dynamic Host Persistence provides persistence of subscriber host information of properties that bind a host to a SAP, an IP address or a MAC address. This provides troubleshooting functionality while avoiding unnecessary and unscalable network queries. Only the properties of the subscriber host which are required to tie the host to other objects for troubleshooting, since there are no statistics and no OAM tests for subscriber hosts, are persisted.

Note — Only IPoE (DHCP and ARP) and IPOE-DHCP6 hosts can be persisted in the 5620 SAM.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Host from the object list.

3 Click on the Search Subscriber Host Information from Last Resynch radio button.

4 View the available read-only attributes.

5 If required, click on the Resync Subscriber Host Table button. The ESM Capable Network Element form opens.

6 Select one or more NEs. Click on the OK button. A dialog box opens.

7 Click on the check box. Click on the Yes button.

8 The Select an ESM Capable Network Element form closes.

9 To retrieve the SAPs on which a subscriber host with an IP address resides, perform the following steps:

Note — You can also retrieve DHCP, PPPoE sessions, and ARP host information on demand from the Manage→Residential Subscribers menu option. The Manage Residential Subscribers form opens.

i Click on the Search Current Subscriber Host Information radio button.

ii Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

iii Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

iv Configure the Service ID parameter.

v Click on the Select button beside Port to specify a port. The Select Port form opens.

vi Select a port in the list and click on the OK button. Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

vii Click on the Search button.

viii View the available read-only attributes.

ix Close the Manage Residential Subscribers form.

Procedure 68-41 To view a subscriber and the associated subscriber hosts

Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services. See chapter 100 for more information.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Properties button. The Residential Subscriber (View) form opens with the General tab displayed.

5 View a list of the residential subscriber instances for the subscriber, if required.

i Click on the Residential Subscriber Instances tab button.

ii Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

iii View the instance information.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

iv Close the Residential Subscriber Instance (Edit) form.

6 Specify the subscribed application profile for AA reporting, if required.

i Click on the Residential Subscriber Instances tab button.

ii Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

iii Configure the Subscribed Application Profile parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button.

7 List and view the active hosts for the subscriber, if required.

i Click on the Subscriber Hosts tab button.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 8.

v View the subscriber host information.

vi Close the Subscriber Host form.

8 Close the Residential Subscriber (View) form.

9 Close the Manage Residential Subscribers form.

Procedure 68-42 To view a subscriber instance and the associated subscriber hosts

Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services. See chapter 100 for more information.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

4 Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

5 List and view the active hosts for the subscriber instance, if required.

i Click on the Subscriber Hosts tab button.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 7.

v View the subscriber host information.

vi Click on the Cancel button to close the Subscriber Host form.

6 List and view the subscriber hosts for which a DHCP lease has been manually terminated, if required.

i Click on the Clear Status tab button.

ii To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 7.

iii View the subscriber host DHCP lease information.

iv Click on the Cancel button to close the Subscriber Host form.

7 View the collected statistics for the subscriber instance, if required.

i Click on the Statistics tab button.

ii Choose a statistics class from the object drop-down list.

iii Click on the Collect button to collect the statistics for the chosen class, or click on the Collect All button to collect the statistics for all classes.

iv Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

v View the statistics information.

vi Click on the Close button to close the statistics record form.

vii Repeat steps ii to vi for each statistics class that you want to view.

8 Click on the Cancel button to close the Residential Subscriber Instance (Edit) form.

9 Close the Manage Residential Subscribers form.

Procedure 68-43 To view or configure active residential subscriber hosts on a SAP

Note — The 5620 SAM does not automatically display a list of all active hosts on a SAP because the number of hosts on a SAP is potentially large and may take a long time to retrieve. You must request the list of hosts on a SAP. The 5620 SAM prompts you for confirmation before retrieving the list of hosts.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to view or configure active residential subscriber hosts on a SAP; expand the entries for that site.

5 Click on the Access Interfaces icon to display the site SAPs.

6 Select a SAP, right-click, and choose Properties. The SAP configuration (Edit) form opens with the General tab displayed.

7 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

8 Click on the Subscriber Hosts tab button.

9 Click on the Find button. A confirmation prompt appears.

10 Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

11 To view the information for a subscriber host, select the host entry and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed.

12 If the subscriber host is a static host, go to step 19.

13 Configure the Subscriber Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose a subscriber profile string from the Subscriber Profile String - Subscriber Host form.

> **Caution —** Changing the subscriber profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one subscriber profile, when you change the subscriber profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new subscriber profile.

14 Configure the SLA Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose an SLA profile from the SLA Profile - Subscriber Host form.

15 Configure the Application Profile parameter for the dynamic host PPPoE host, if required. Click on the Select button to choose an application profile string from the Application Profile String - Subscriber Host form.

> **Caution —** Changing the application profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one application profile, when you change the application profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new application profile.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Subscriber Host form closes.

18 Go to step 20.

19 Click on the Cancel button to close the Subscriber Host form.

20 Click on the OK button. The SAP configuration form closes.

21 Close the Manage Services form.

Procedure 68-44 To view SHCV log events

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose SHCV Event Log from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

5 Select a log entry and click on the Properties button. The SHCV Log Entry form opens.

6 View the log entry.

7 Close the SHCV Log Entry form.

8 Close the Subscriber Host Connectivity Verification form.

9 Close the Manage Residential Subscribers form.

Procedure 68-45 To change the identification of a subscriber

Perform this procedure to change the identification of a subscriber, for example, when you no longer want hosts on the SAP to use the SAP ID as the subscriber ID.

Caution 1 — Renaming a subscriber can be service-affecting because it changes the subscriber identification string of all associated subscriber hosts. Before you proceed, ensure that no subscriber hosts require the subscriber identification string associated with this subscriber.

Caution 2 — Renaming a subscriber changes the SAP default subscriber identification strings that are associated with it.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Modify button. The Residential Subscriber (Edit) form opens with the General tab displayed.

5 Configure the New Subscriber Identification parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM renames the subscriber.

8 Close the Manage Residential Subscribers form.

Procedure 68-46 To reset a subscriber's subscription credit limit

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form appears.

2 Choose Residential Subscriber Host from the Object Type drop-down list.

3 Click on the Search button. A list of residential subscriber hosts is displayed.

4 Perform one of the following:

  a Select a host from the list and click on the Reset Credit button. Go to step 9.

  b Select a host from the list and click on the Properties button. The Subscriber Host form opens.

5 Click on the Credit Control Operational values tab button.

6 Select an entry from the list and perform one of the following:

  a Click on the Reset Credit button. Go to step 8.

  b Click on the Properties button. A form opens.

7 Close the form after viewing credit control data.

8 Close the Subscriber Host form.

9 Close the Manage Residential Subscribers form.

Procedure 68-47 To modify the primary subscriber identification script or URL

This procedure allows a 5620 SAM operator to modify the primary subscriber identification script without service disruption. Perform this procedure only when the primary script and URL are operational.

Caution — Modifying the primary subscriber identification script is potentially service-affecting if no functional backup script is administratively enabled. Modifying a backup (secondary or tertiary) subscriber identification script is unlikely to be service-affecting if the other backup script (secondary or tertiary) functions properly and is administratively enabled. Ensure that at least one administratively enabled backup script is accessible to the 5620 SAM and the NEs to which it applies before you proceed.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose Subscriber Identification Policy from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.

4 Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens with the General tab displayed.

5 Copy the operational primary script URL to the secondary position. This action ensures that an operational backup script is in place in the event that there is a problem with the new primary script or URL.

- **i** Set the Secondary Script Administrative State parameter to disabled.
- **ii** Click on the Apply button. A dialog box appears.
- **iii** Click on the Yes button. The 5620 SAM administratively disables the secondary script.
- **iv** Configure the Secondary Script URL parameter with the value of the Primary Script URL parameter.
- **v** Set the Secondary Script Administrative State parameter to enabled.
- **vi** Click on the Apply button. A dialog box appears.
- **vii** Click on the Yes button. The 5620 SAM administratively enables the secondary script.

Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

6 Modify a renamed copy of the former primary script or create a replacement script, as required; record the new or modified script URL.

7 Configure the new URL as the primary script URL.

i Set the Primary Script Administrative State parameter to Disabled.

ii Click on the Apply button. A dialog box appears.

iii Click on the Yes button. The 5620 SAM administratively disables the primary script. The secondary (former primary) script is the active script.

iv Configure the Primary Script URL parameter with the new URL value.

v Set the Primary Script Administrative State parameter to Enabled.

vi Click on the Apply button. A dialog box appears.

vii Click on the Yes button. The 5620 SAM administratively enables the primary script. The new primary script is the active script.

Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Subscriber Identification Policy (Edit) form closes.

10 Close the Manage Subscriber Policies form.

Procedure 68-48 To delete an inactive residential subscriber instance

Use this procedure to remove the record of an inactive residential subscriber instance from the 5620 SAM database. Residential subscriber instances become inactive in the 5620 SAM when the subscriber is deleted from the NE.

Note — AA statistics data can be lost when you delete a residential subscriber instance before the 5620 SAM is finished collecting and processing AA statistics. Alcatel-Lucent recommends waiting at least two statistics collection intervals before deleting an inactive residential subscriber instance.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

The Active property indicates the status of each residential subscriber instance in the list. An inactive residential subscriber instance has no check mark under the Active heading.

4 Select the inactive residential subscriber instance you want to delete and click on the Delete button. The inactive residential subscriber instance is removed from the list.

5 Close the Manage Residential Subscribers form.

69 — VLAN service management

69.1 VLAN service management overview

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. Table 69-1 lists the types of VLAN services that are supported on the 5620 SAM by device type:

Table 69-1 Device VLAN support

Device	Supported VLAN types
7250 SAS 7250 SAS-ES 7250 SAS-ESA 7450 ESS Telco	• Standard VLAN • Management VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN • Super (Internet Access) VLAN
All OmniSwitches except for the OS 6900 and OS 10K	• Standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN
9500 MPR	• 9500 MPR (dot1q) VLAN

Several 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, 7450 ESS, Telco, 9500 MPR and OmniSwitch VLAN services can be interconnected through a backbone VPLS.

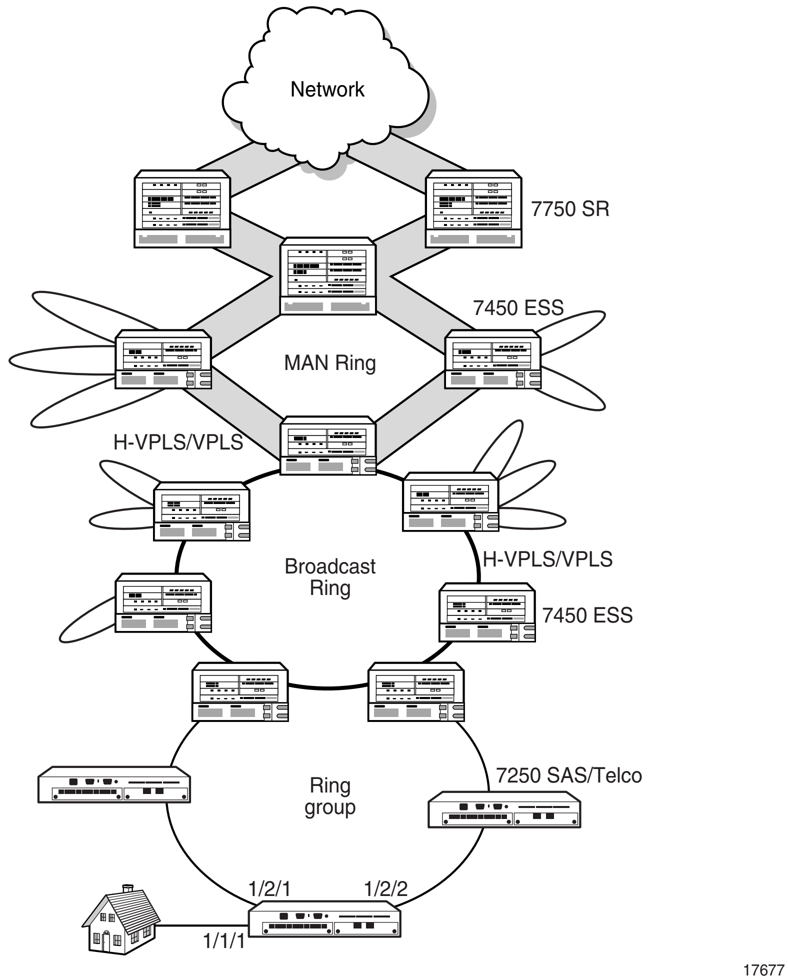
The 5620 SAM supports end-to-end VLAN configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

VLAN ring groups

VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, from a 7450 ESS, to all devices in the ring. STP configuration on OmniSwitch, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices ensures that there is a constant stream of traffic in either direction by rerouting traffic around breaks in the physical links between the devices. Figure 69-1 shows an example of a ring group that is part of a larger metropolitan area network. The scenario shown in Figure 69-1 also supports OmniSwitch NEs instead of the 7250 SAS/Telco NEs shown.

Figure 69-1 Ring in a metropolitan and broadcast network



The 5620 SAM provides OAM tools for service validation and for troubleshooting service and network transport issues.You can run the OAM Validation test suite for the VLAN service by clicking on the More Actions > Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays more detailed information about the OAM test result. See chapter 78 for more information about how to configure OAM validation test suites.

The Aggregated Service Site Operational State parameter has four possible values. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State parameter is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 76 for more information about the hierarchical organization of composite services.

VLAN groups and paths

The 5620 SAM supports the configuration and provisioning of VLAN groups and paths which are used by the following NEs.

- OmniSwitch devices (VLAN groups only) to configure VLAN services
- 9500 MPR ANSI/ETSI (2.x and 3.x streams) to configure VLAN and VLL services

VLAN groups

You can use VLAN groups to:

- logically group OmniSwitch and 9500 MPR devices to represent a typical network topology. An OmniSwitch and a 9500 MPR cannot belong to the same VLAN group.
- manage the VLAN IDs that are assigned to 9500 MPR VLAN group members.

Note — When you create a 9500 MPR service, they can only be configured between 9500 MPRs that belong to the same VLAN group.

See Procedure 69-10 for more information about creating VLAN groups.

VLAN paths

A VLAN path is a bidirectional transport-tunnel service that is used to support alarm correlation and to turn up radio backhaul services on 9500 MPR devices. VLAN paths use a tree or mesh topology. The paths can span NEs that are connected by both radio links and physical links. You can configure a VLAN path as follows:

- Ring based—An ERP topology is a collection of Ethernet ring nodes that form a closed physical loop. Each Ethernet ring node is connected to two adjacent Ethernet ring nodes via a duplex communications facility. An Ethernet ring can contain a minimum of 2 Ethernet ring nodes and a maximum of 16.
- Hop based—Users specify the number of hops from a source 9500 MPR to a destination 9500 MPR. Each hop in the path is a 9500 MPR that belongs to the same VLAN group.The following hop-based VLAN paths variants are supported.
    - Auto—A user defines the head end of the VLAN group, the hops the VLAN path takes, and optionally, the minimum bandwidth requirements, and whether the shortest path should be used. The 5620 SAM determines the appropriate available route for the VLAN path.
    - Manual—A user defines the source 9500 MPR, the hops and links the VLAN path takes, and optionally, the minimum bandwidth requirements.
    - Point 2 Point—A user defines the source and destination 9500 MPR, the maximum number of allowed hops and, optionally, the minimum bandwidth requirements, and whether the shortest path should be used.

See Procedure 69-12 for more information about creating VLAN paths.

VLAN service policies (7250 SAS, 7450 ESS, and Telco)

Policies can be assigned to ports on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices. Policies are defined at a global level and then applied to components of the service, such as a port.

Note — The 5620 SAM supports the distribution of policies on the 7450 ESS, 7750 SR, 7710 SR, Release 6.3 or earlier Telco devices, and on the 7250 SAS and 7250 SAS-ES, prior to Release 2.0.

The policy on the component is then a local version of the global policy. The following policies are common to VLAN services:

- QoS policies define ingress classification, policing, shaping, and marking on the device. QoS policies are configured using the Telco Qos Node Level Policy Manager.
- Filter policies control network traffic into or out of an interface or device based on IP or MAC matching criteria. Filter policies are configured using the Telco ACL Standard IP Filter Manager, the Telco ACL Extended IP Filter Manager, and the Telco ACL MAC Filter Manager.
- Multicast policies define the available broadcast addresses (BTV channels) for a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco ring. ACL IGMP filters specify the filters that are applied for end users to the channels to ensure that only the subscribed channels are delivered. Multicast polices and filters are configured using the Multicast Package Policy Manager and the Telco ACL IGMP Filter Manager, and are applied during service creation.

See chapter 46 for more information about policies.

VLAN service policies (OmniSwitch)

Policies can be assigned to ports on an OmniSwitch. Policies are defined at a global level and then applied to components of the service, such as a port.

The policy on the component is then a local version of the global policy. The following policies are common to VLAN services:

- QoS policies define ingress classification, policing, shaping, and marking on the device.
- UNI policies define how control frames that are received on a port are processed. UNI policies are applied to a port that is used as a SAP in a L2 VPN TLS (stacked) VLAN.
- SAP policies define traffic engineering parameters for bandwidth sharing, rate limiting, CVLAN translation (or double-tagging), and priority bit mapping. SAP policies are applied to the service access multi-point.
- Filter policies control network traffic into or out of an interface or device based on IP or MAC matching criteria.

See chapter 46 for more information about policies.

Default VLANs

By default, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices (except for the OS 6900 and OS 10K) are configured with a default VLAN that uses VLAN ID 1. In addition, access ports on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA are untagged and configured for access mode as members of VLAN ID 1.

Note — The 5620 SAM does not manage VLAN ID 1 on an OmniSwitch.

Before you create a VLAN on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA, device using untagged ports, ensure the following.

- Renumber the default VLAN (ID 1) with the new VLAN ID that you want to use.
- Remove all untagged access ports that are not members of the new VLAN.
- Do not share untagged ports between VLANs, as there can only be one default VLAN for each untagged port.

See section 20.2 for more information about tagged and untagged ports.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management

The 5620 SAM manages the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices (except for the OS 6900 and OS 10K) using SNMP and CLI messages. The devices support termination of all VLAN types on Ethernet ports. The 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA supports the termination of standard VLANs and L2 VPN VLANs on CES ports with dot1q encapsulation.

When using 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices to ensure the latest management view of the network, a management VLAN must be created on devices that belong to a ring group. This is done by:

- ensuring ports are configured to allow management message traffic
- making the 7450 ESS part of a management VPLS, used to relay SNMP and CLI messages to the devices

Spanning tree protocols

The STP configuration on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device in a ring group or an OmniSwitch device (except for the OS 6900 and OS 10K) in a VLAN group detects loops in the topology and ensures that there is a constant stream of traffic by rerouting traffic around breaks in the physical links between the devices. The 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices support STP, MSTP and RSTP.

Spanning tree on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices

Spanning tree protocols are a global configuration, and only one protocol can be enabled at a time. For example, if you enable RSTP while STP is already running, the 7250 SAS disables STP and runs RSTP. You can disable STP per port when MSTP or RSTP is enabled globally. Spanning tree protocols must be configured before the 5620 SAM manages the device.

Spanning tree on OmniSwitch devices

The OmniSwitch can operate in the following spanning tree modes:

- flat
- 1 x 1

The flat mode provides a CST instance that applies across all VLANs and supports STP (802.1D), RSTP (802.1w), and MSTP. MSTP allows the mapping of one or more VLANs to a single spanning tree instance.

The 1x1 mode is an Alcatel-Lucent proprietary implementation that automatically calculates a separate spanning tree instance for each VLAN configured on the switch. This mode only supports the use of the STP and RSTP.

By default, an OmniSwitch runs in the 1x1 mode and uses the 802.1D protocol.

The 5620 SAM supports the configuration of Spanning Tree protocols and modes.

See the OmniSwitch user documentation for more information about Spanning Tree modes.

STP

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. Fault-tolerant internetworks must have a loop-free path between all the nodes in a network. The spanning tree algorithm calculates the best loop-free path through a switched Layer 2 network. Switches send and receive STP frames at regular intervals but do not forward these frames.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch user documentation for more information about device-specific STP CLI commands and parameters.

RSTP

RSTP uses point-to-point wiring to provide rapid convergence of the spanning tree. With RSTP, the spanning tree may be reconfigured in less than 1 s, as compared to 50 s required with the default STP settings. This is critical in networks that carry voice, video, and other delay-sensitive traffic.

RSTP assigns port roles and determines the active topology to provide rapid convergence of the spanning tree. RSTP selects the switch with the highest switch priority.

See the 7250 SAS, Telco, and OmniSwitch user documentation for more information about device-specific RSTP CLI commands and parameters.

MSTP

MSTP allows you to group and associate VLANs to multiple spanning tree instances, or forwarding paths. MSTP allows up to 16 RSTP instances to be run and associates a VLAN with a specific MST instance. This reduces link convergence time and enables load balancing over a large number of VLANs.

Each MST instance can have its own independent topology. Multiple forwarding paths improve network fault tolerance because when one instance fails, data flow is unaffected over the remaining forwarding paths. You can manage large networks and use redundant paths more easily by allocating different VLAN and spanning tree instance assignments to different parts of the network.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch user documentation for more information about device-specific RSTP CLI commands and parameters.

MSTP fast ring (7250 SAS and Telco only)

The MSTP fast ring mode shortens the MSTP convergence time in a ring topology when a disconnection occurs. To use MSTP fast ring, you must select one bridge to be the root bridge by setting its priority to the lowest value. All of the user ports must be configured as MSTP edge ports.

To optimize the performance of your network, increment the priority of the bridges as you draw away from the root bridge.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco user documentation for information about configuring the MSTP fast ring.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, 7210 SAS-M and Telco VLAN restrictions

VLANs with the characteristics listed in either of the following scenarios cannot be modified using the 5620 SAM. A deployment error results when you attempt to modify the VLAN.

Scenario 1

- the VLAN was not created using the 5620 SAM
- the VLAN name contains more than 19 characters

Scenario 2

- the VLAN was created using the 5620 SAM
- the VLAN contains more than 19 characters
- the VLAN was removed from the 5620 SAM database because of the unmanaging and remanaging of a node or the deletion of a service
- the nodes that are part of the VLAN were rediscovered

9500 MPR services

A 9500 MPR service is created by configuring sites and access interfaces, and then associating the service with a VLAN path. The 5620 SAM creates cross-connects between the physical ports on all 9500 MPRs along the VLAN path. These paths with cross-connects are called VLAN path instances. VLAN path instances are specific to a service, and each VLAN service will have its own underlying VLAN path instance. A VLAN path can have multiple VLAN path instances. The VLAN path instance and all of the cross-connects on the service can be viewed along with other service properties.

All 9500 MPR services use the default customer and are identified by a VLAN ID assigned at each inflow interface and a service ID. The service ID and VLAN ID have different values.The VLAN ID can be automatically assigned by the 5620 SAM or assigned by the user. When the 5620 SAM assigns the VLAN ID, the ID is based on the VLAN group that the endpoint 9500 MPR belongs to.

You can configure the following service types on the 9500 MPR:

- 9500 MPR (dot1q) VLAN services; see Procedure 69-8.
- VLL services; see chapter 70.
    - Epipe (ANSI)
    - Apipe (ETSI)
    - Cpipe (ANSI and ETSI)
- Composite services; see chapter 76.

Service-in-service automatic discovery

The 5620 SAM supports automatic discovery for service-in-service associations created with the 9500 MPR. Service-in-service refers to a transport service which carries services for network routers. Automatic discovery allows the 5620 SAM to automatically associate a transport service with a service tunnel when a physical link is created between the 9500 MPR and a non-MPR NE. Service faults generated on either of the associated services will become cross-correlated in the 5620 SAM.

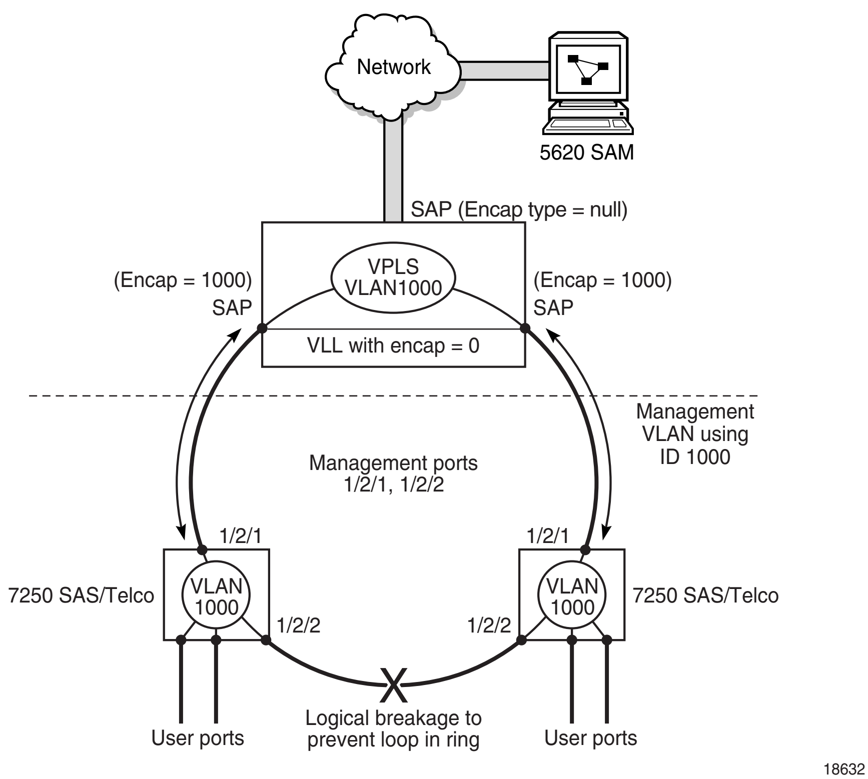
Note 1 — Service-in-service automatic discovery will not overwrite a service which is already associated with a service tunnel. Users can, however, manually overwrite an automatic association with another service. Only one service can be associated to a service tunnel. Refer to Chapter 33 for mote information on associating a service to a service tunnel.

Note 2 — If the physical link between the 9500 MPR and the network router is removed, the 5620 SAM will automatically disassociate the service from the service tunnel.

69.2 Sample management VLAN configuration

Figure 69-2 shows a sample management VLAN service configuration. The configuration depends on the specific network requirements.

Figure 69-2 Sample management VLAN



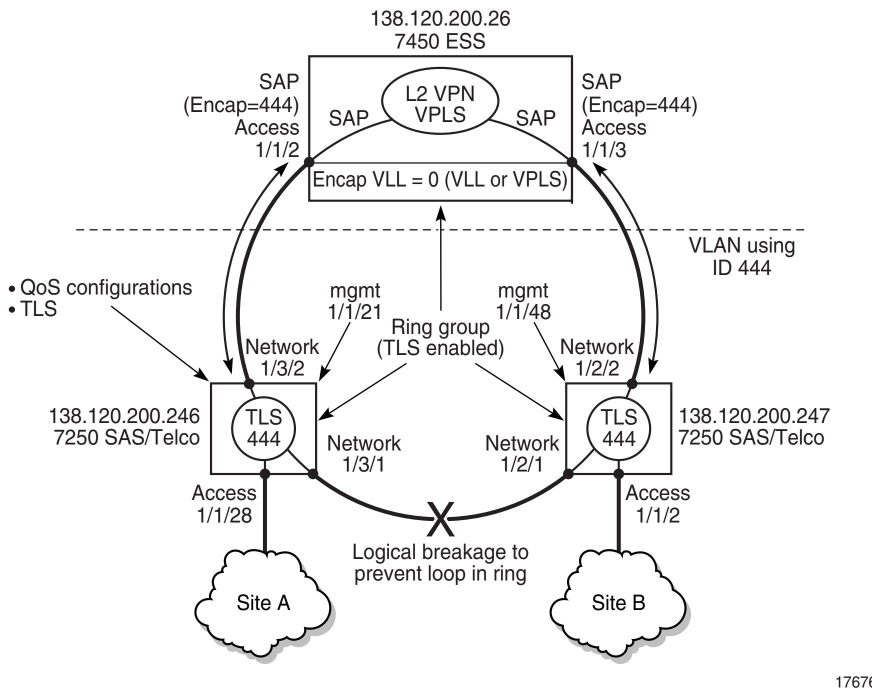
The following high-level steps describe the configuration of the sample management VLAN.

1 Choose a management VLAN ID to be used in the ring, for example, ID 1000.
2 Create a VPLS on the 7450 ESS that has the SAPs in the VPLS set with encapsulation 1000. See chapter 71 for more information about creating a VPLS.
3 The port to which the 5620 SAM is connected to the network is added to the VPLS without encapsulation.
4 Create a management VLAN on each 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device; for example, by using CLI:
    - config vlan
    - create mgt_1000
    - config mgt_1000
    - add ports 1/2/1, 1/2/2 tagged
5 Exclude all other VLANs from being management VLANs, for example, by using CLI:
    - config vlan
    - no management 1-999,1001-4094 (for a Telco) no management 1-999, 1001-4092 (for a 7250 SAS)
6 Ensure only the uplink ports from the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices have device management capabilities to ensure user ports cannot access CLI, SNMP, or FTP functionality, for example, by using CLI:
    - config
    - no port management 1/1/1-1/1/24

69.3 Sample L2 VPN VLAN configuration

Figure 69-3 shows a sample L2 VPN VLAN service configuration. Transparent LAN services such as a L2 VPN are used to transport large numbers of customer VLANs while keeping the traffic in each VLAN segregated. The configuration depends on the specific network requirements.

Figure 69-3 Sample L2 VPN VLAN configuration



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS or Telco devices.
    - pre-discovery CLI modifications
    - discovery including mediation configuration with the CLI user names and passwords
    - configure protocol to manage topology loops, such as MSTP or RSTP
- Ensure that the TLS VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs must match the VLAN ID of the ring VLAN.
- Configure the 7250 SAS or Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- Configure the bridge instances for the 7250 SAS or Telco devices from the network view in the navigation tree.
- Devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.
- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
    - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
    - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
    - A L2 VPN VPLS is created on the 7450 ESS.

Table 69-2 lists the high-level tasks that are required to configure this sample VLAN L2 VPN service.

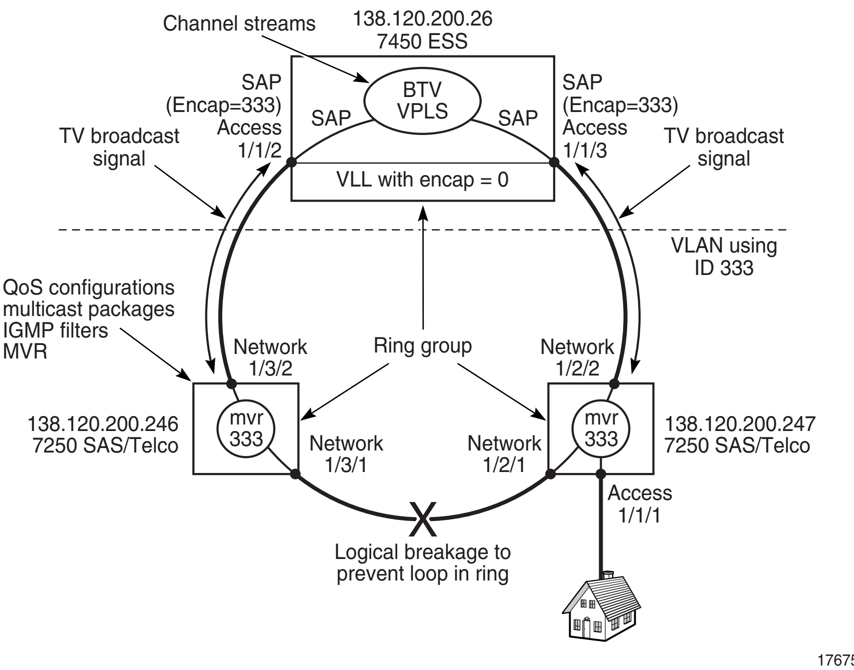
Table 69-2 Sample VLAN L2 VPN service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creating of ring groups that are enabled to receive TLS (L2 VPN) streams: • The ring group contains all three devices. • TLS is enabled for the ring group. • Ports 1/3/1 and 1/3/2 on the device connected to Site A and 1/2/1 and 1/2/2 connected to Site B are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS, and the encapsulation matches the VLAN ID (444). • Ports 1/1/2 and 1/1/28 on the 7250 SAS and Telco devices are configured as access ports.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the 7250 SAS and Telco devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. The policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

69.4 Sample BTV VLAN configuration

Figure 69-4 shows a sample broadcast TV VLAN configuration. BTV VLANs are shared VLANs, where the multicast broadcast channels or pay per view channels are available across the ring, and based on subscriptions and privileges determined using IGMP snooping, the user gains or is denied access. The configuration depends on the specific network requirements.

Figure 69-4 Sample BTV VLAN configuration



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices:
    - pre-discovery CLI modifications
    - SNMP trap forwarding to the 5620 SAM
    - discovery, including mediation configuration with the CLI user names and passwords
    - configure protocols to manage topology loops, such as MSTP or RSTP
- Ensure that the BTV VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs should match the VLAN ID of the ring VLAN.
- Configure 7250 SAS and Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- Configure the bridge instances for the 7250 SAS and Telco devices from the network view in the navigation tree.
- Enable IGMP snooping on the bridge instance for the 7250 SAS and Telco devices included in the broadcast TV VLAN.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
    - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
    - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
    - A BTV VPLS is created on the 7450 ESS.
- Create and manage the necessary broadcast TV policies, including multicast package and IGMP filtering.

Table 69-3 lists the high-level tasks that are required to configure this sample broadcast TV VLAN service.

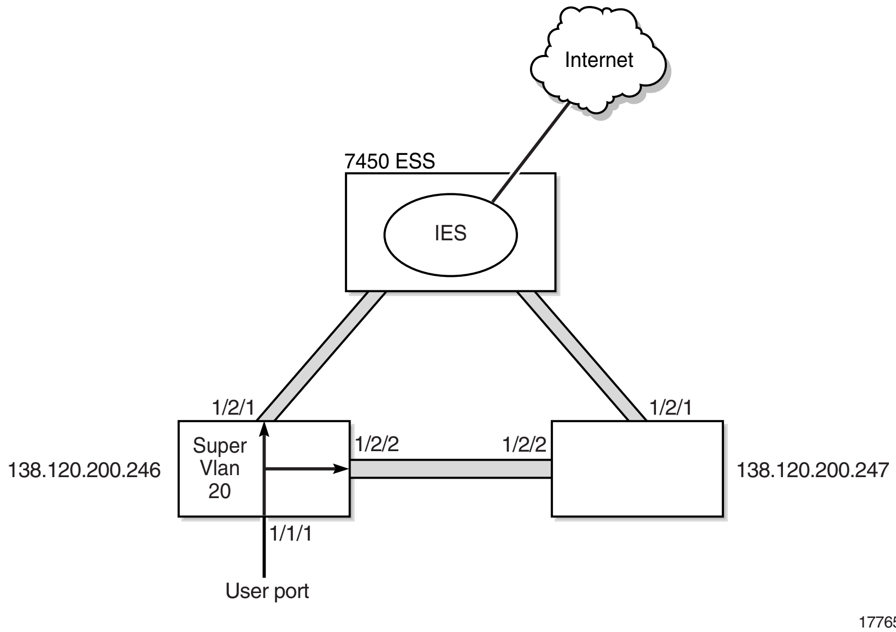
Table 69-3 Sample broadcast TV VLAN service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creation of ring groups: • The ring group contains all three devices. • Ports 1/3/1 and 1/3/2 on the device with the IP address 138.120.200.246 and ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.247 are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS with an encapsulation matching the VLAN ID (333). • Port 1/1/1 on device 138.120.200.247 is configured as access.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN BTV service. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the 7250 SAS and Telco devices in the ring • multicast package policies to determine the content of the broadcast streams that are sent to the 7250 SAS and Telco devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. Policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms: Ensure that the VLAN created for the ring group uses ID 333.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. You use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

69.5 Sample super VLAN configuration

Figure 69-5 shows a sample super VLAN configuration. Super VLANs are used to restrict traffic that arrives on the user port to the uplink port. This disallows traffic between user ports. This application is often used for public Internet access services. The configuration depends on the specific network requirements.

Figure 69-5 Sample super VLAN configuration



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices:
    - pre-discovery CLI modifications
    - SNMP trap forwarding to the 5620 SAM
    - discovery, including mediation configuration with the CLI user names and passwords
    - configure protocol to manage topology loops, such as MSTP or RSTP
- Ensure that the 7450 ESS is configured to support super VLAN Internet access.
- Create an IES on the 7450 ESS.
- Configure 7250 SAS and Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

Table 69-4 lists the high-level tasks that are required to configure this sample super VLAN service.

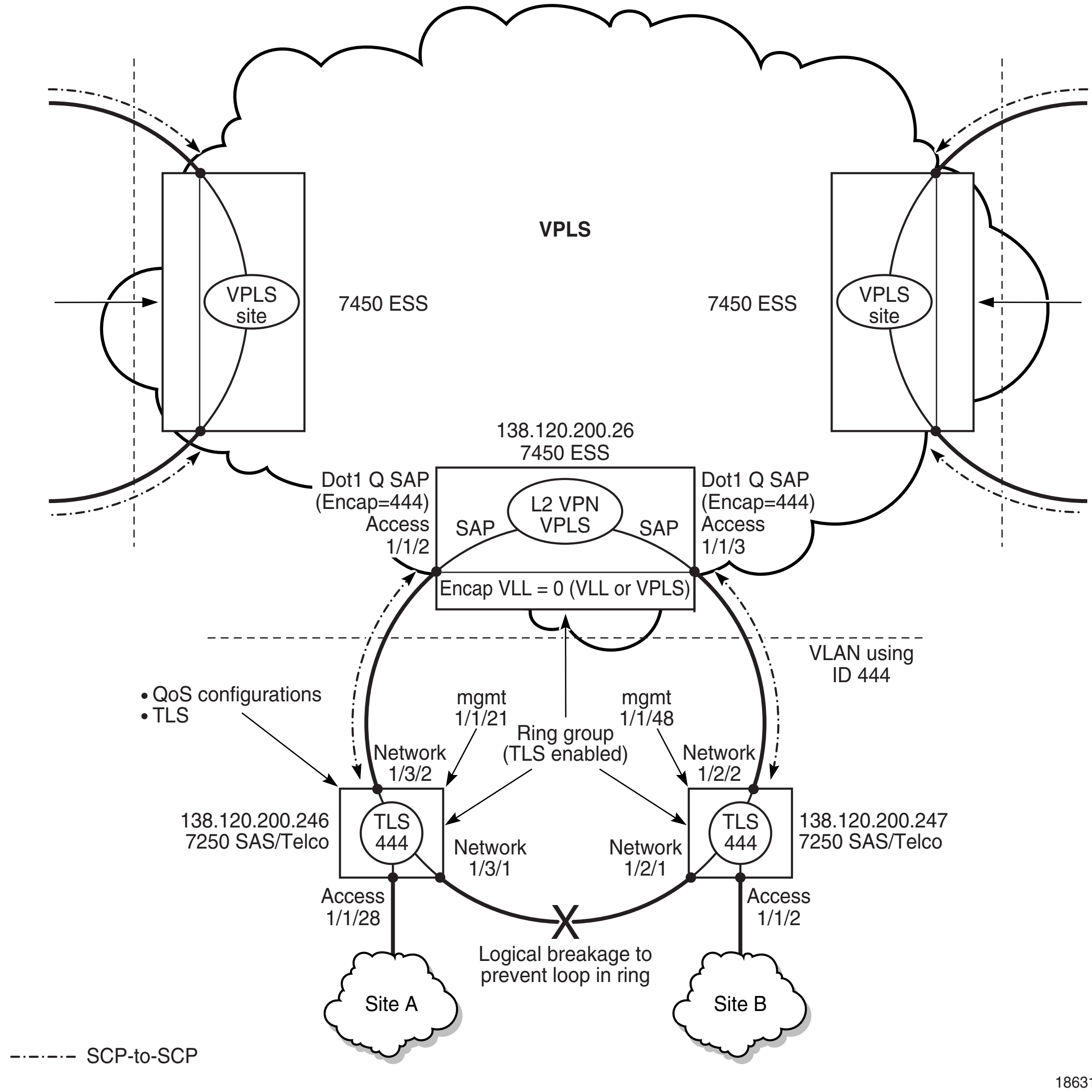
Table 69-4 Sample configuration for a super VLAN

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creation of ring groups: • The ring group contains all three devices. • Ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.246 and ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.247 are configured as network to act as uplinks. • Port 1/1/1 on device 138.120.200.246 is configured as access.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a super VLAN service. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies
3. Distribute policies to devices	Distribute configured policies to the devices. Policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms: • The super VLAN created for the ring group uses ID 20.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

69.6 Sample interconnection VLAN configuration

Figure 69-6 shows a sample configuration of an interconnection of VLANs across a VPLS backbone.

Figure 69-6 Sample interconnection VLAN



Verify that the following preconfigurations are complete:

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices.
    - pre-discovery CLI modifications
    - SNMP trap forwarding to the 5620 SAM
    - discovery including mediation configuration with the CLI user names and passwords
    - ports are configured as access (ports that are part of the VLAN) and network (ports that are used for uplinks)
    - configure protocol to manage topology loops, such as MSTP or RSTP, using CLI

- Configure 7250 SAS and Telco ports as access and network, as required, from the navigation tree.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

Table 69-5 lists the high-level tasks that are required to configure this sample interconnection of VLAN services.

Table 69-5 Sample VLAN interconnection configuration

Task	Description
1. Manage and configure	Ensure that the required configurations are completed to equipment as described in Table 69-2, including the following. • configuring access and network ports • enabling CLI configuration on managed 7250 SAS and Telco devices • creating ring groups that are enabled to receive TLS (L2 VPN) streams • configuring and distributing policies
2. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
3. Configure VPLS	Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS matches the VLAN ID of each VLAN service in the ring group. Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS at each VPLS site is Dot1 Q. See chapter 71 for more information about creating a VPLS.
4. Create composite service	Create a composite service to interconnect the VLAN services with the VPLS. • Create the composite service. • Define general properties for the composite service. • Specify the services that are participating in the composite service. You can specify multiple services in one operation. • Create SCP-to-SCP connectors to link the dot1q-encapsulated VPLS SAP and the adjacent L2 switch uplinks of the VLAN ring group. See chapter 76 for more information about creating composite services.

69.7 Workflow to create VLAN services (7250 SAS, 7450 ESS, Telco, and 9500 MPR)

The following workflow lists the high-level steps required to create a VLAN service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and 9500 MPR devices. As a prerequisite for creating a VLAN service, this workflow assumes that the following appropriate preconfigurations have been performed:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI user name and password
- configuration of protocol to manage topology loops, such as MSTP or RSTP.
- ensure the TLS or BTV VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs should match the VLAN ID of the ring VLAN.

- Configure 7250 SAS and Telco ports as Access and Network, as required, from the navigation tree.
- Configure the bridge instances for the 7250 SAS and Telco devices from the network view in the navigation tree, as described in chapter 31.
- Create and add devices connected to the 7450 ESS as part of a ring group, as described in chapter 17.
- Set up customers or associate existing customers with the new service; see chapter 9 for more information.
- Policies should be configured before you create a service. The following key policies can be applied as required, to resources that are part of a VLAN service. See chapter 46 for more information.
    - QoS policies for the 7250 SAS and Telco devices and ports
    - scheduling policies
    - filter policies, including IGMP filter policies to create and deploy access control lists on the 7250 SAS and Telco devices in the ring
    - multicast package policies to determine the content of the broadcast streams that are sent to the 7250 SAS and Telco devices in the ring
- Ensure that the required configurations are completed on equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creation of ring groups that are enabled to receive TLS (L2 VPN) streams. See Table 69-2, 69-3, or 69-4 for the high-level equipment tasks that are required to configure a VLAN.

1 Distribute configured policies to the devices. The policies are used during the creation of VLAN services. See Procedure 46-1.

2 Provision the VLAN service.

a For Standard VLANs, see Procedure 69-1.

- Set the application parameter to Standard VLAN.

b For Management VLANs, see Procedure 69-2.

- Set the application parameter to Management VLAN.

c For L2 VPN TLS VLANs, see Procedure 69-3.

- Set the application parameter to L2-VPN (TLS/VLAN-Stacking).
- Ensure that the VLAN created for the ring group uses ID 444.

d For BTV VLAN s VLANs, see Procedure 69-5.

- Set the application parameter to Broadcast TV (MVR/IPMV).
- Ensure that the VLAN created for the ring group uses ID 333.

e For Super VLANs, see Procedure 69-7.

- Set the application parameter to Internet Access (Super-VLAN).
- Ensure that the VLAN created for the ring group uses ID 20.
- Ensure the IES that provides Internet access to the ring VLAN service is configured on the 7450 ESSs.

f For 9500 MPR (dot1q) VLANs, see Procedure 69-8.

- Set the application parameter to 9500 MPR.

3 Associate access interfaces (similar to SAPs) with the VLAN services. These are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users. See Procedure 69-9.

4 For services created on a 9500 MPR, as required:

a Create VLAN groups and add members to each group. See Procedure 69-10.

b Delete a VLAN group or group member. See Procedure 69-11.

c Create the VLAN paths that are required between the 9500 MPR group members. The VLAN path can be hop based or ring based. See Procedure 69-12.

d Delete a 9500 MPR VLAN path. See Procedure 69-13.

5 Turn up the service.

Network interface VLAN bindings are created between the newly created VLAN and all of the network ports on the node.

6 As required, run an OAM validation test on a VLAN service. See Procedure 69-16.

7 As required, view VLAN information:

a View the VLAN service operational status. See Procedure 69-17.

b View the service topology map associated with a VLAN service. See Procedure 69-18.

8 As required, modify a VLAN service. See Procedure 69-19.

9 As required, delete a VLAN service. See Procedure 69-20.

69.8 Workflow to create VLAN services (OmniSwitch)

The following workflow lists the high-level steps required to create a VLAN service on OmniSwitch devices (with the exception of OS 6900 and OS 10K devices). As a prerequisite for creating a VLAN service, this workflow assumes that the following appropriate preconfigurations have been performed:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI usernames and passwords
- addition of the OmniSwitches that participate in the VLAN to a VLAN group

- configure OmniSwitch network ports, as required, from the navigation tree. The Automatic VLAN Binding parameter associated with a network port or LAG must be enabled before the 5620 SAM can identify the network port or LAG as a network interface.
- configure QoS policies, as required.
- configure the bridge instances for the OmniSwitches from the network view in the navigation tree.
- set up customers or associate existing customers with the new service; see chapter 9 for more information.

1 Provision a Standard VLAN service. See Procedure 69-1.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to Standard VLAN.

ii Add sites that are participating in this VLAN. Configure STP and VLAN properties, as required.

iii Create VLAN access interfaces to be used for this service. Specify the access port to be used by each interface and whether the access is tagged.

2 Provision a L2 VPN TLS VLAN service. See Procedure 69-4.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to L2-VPN (TLS/VLAN-Stacking).

ii Add devices connected as part of a VLAN group to the VLAN.

iii Add sites that are participating in this VLAN. Configure STP and VLAN properties, as required.

iv Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

v Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created.

vi Create SAPs. Specify the port to be used as a customer-facing port (UNI).

vii Create CVLANs to associate customer traffic with a VLAN-stacking SAP. CVLANs identify the type of customer traffic that is received on the SAP UNI ports.

3 Provision a BTV VLAN service. See Procedure 69-6.

i Create the VLAN and associate a customer with the VLAN. Set the application parameter to Broadcast TV (MVR/IPMV).

ii Add devices connected as part of a VLAN group, to the VLAN.

iii Create an L2 access interface. The interface acts as the receiver port on the IPMV. The port that is selected must already be used as a SAP in a SVLAN.

iv Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

- **v** Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created.
- **vi** Create SAPs. Specify the port to be used as a customer-facing port (UNI). The UNI port must already be configured as a receiver port on the IP multicast VLAN.
- **vii** Create CVLANs that will be used to associate customer traffic with a VLAN stacking SAP. CVLANs identify the type of customer traffic received on the SAP UNI ports. The service processes and tunnels the traffic through the SVLAN.
- **viii** Add multicast group addresses to the IP multicast VLAN site.
- **ix** Add CVLAN tags to the IP multicast VLAN site. CVLAN tags are used to bind IP multicast VLANs to a receiver port.

4 Associate access interfaces (similar to SAPs) with the VLAN services. These are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users. See Procedure 69-9.

5 For services created on a OmniSwitch, as required:

- **a** Create VLAN groups and add members to each group as required. See Procedure 69-10.
- **b** Delete a VLAN group or group member. See Procedure 69-11.
- **c** Add a MEP to an OmniSwitch VLAN service access interface. See Procedure 69-14.
- **d** Configure IGMP on an OmniSwitch VLAN site. See Procedure 69-15.

6 Turn up the service.

Network interface VLAN bindings are created between the newly-created VLAN and all of the network ports on the node.

7 As required, run an OAM validation test on a VLAN service. See Procedure 69-16.

8 As required, view VLAN information:

- **a** View the VLAN service operational status. See Procedure 69-17.
- **b** View the service topology map associated with a VLAN service. See Procedure 69-18.

9 As required, modify a VLAN service. See Procedure 69-19.

10 As required, delete a VLAN service. See Procedure 69-20.

69.9 VLAN service management procedures

Use the following procedures to perform VLAN creation and management tasks.

Procedure 69-1 To create a standard VLAN service

Perform the following procedure to create a standard VLAN service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices.

Note — Alcatel-Lucent recommends that you specify the OmniSwitch ports that will be network interfaces before you configure a standard VLAN service.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information displayed in the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State
  This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Set the Application parameter to Standard VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form appears with the site information displayed on the General tab.

11 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

12 Perform one of the following actions:

a If you are configuring a standard VLAN on an OmniSwitch, go to step 13.

b If you are configuring a standard VLAN on a 7250 SAS or Telco device, go to step 15.

13 Click on the VLAN tab button.

14 Configure the parameters:

- Enable Mobile-Tag
- Enable Authentication

15 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

16 Configure the parameters.

- Description
- Administrative State

17 Click on the Port tab button.

18 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

19 Use the configurable filter and Search button to choose a port for user-side access to the VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

20 Click on the VLAN tab button.

21 Configure the VLAN Tagging parameter. The parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created, the parameter cannot be modified. If you need to change the value of this parameter, you must first delete the SAP and create a SAP that matches the new requirements.

22 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

23 Click on the OK button. The Site (Create) form reappears.

24 Repeat steps 15 to 23 for each access interface that you need to create on the site.

25 Perform one of the following actions:

- If you are configuring a standard VLAN on an OmniSwitch, go to step 26.
- If you are configuring a standard VLAN on a 7250 SAS or Telco device, go to step 24.

26 Click on the STP tab button.

27 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

28 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

29 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

30 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

31 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

32 Click on the OK button. The DHCP Snooping General tab reappears.

33 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

34 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

35 Configure the MAC Address parameter.

36 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

37 Choose a port from the list and click on the OK button.

38 The DHCP Snooping Binding Database (Create) form reappears.

39 Configure the parameters:

- IP Address
- Lease Time

40 Click Apply to add the static entry to the table. A dialog box appears.

41 Click on the OK button.

42 Repeat steps 33 to 41 for each static entry that you need to add to the binding table.

43 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

44 Click on the OK button. The Site (Create) form reappears.

45 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed.

46 Click on the OK button to close the VLAN (Create) form.

Procedure 69-2 To create a management VLAN service

Perform the following procedure to create a management VLAN service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Services form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the management VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the management VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State

This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Set the Application parameter to Management VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the management VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form reappears with the site information displayed on the General tab.

11 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

12 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

13 Configure the parameters.

- Name
- Description
- Administrative State

14 Click on the Port tab button.

15 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

16 Use the configurable filter and Search button to choose a port for user-side access to the management VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

17 Configure the remaining parameters, if required.

18 Click on the VLAN tab button.

19 Configure the VLAN Tagging parameter. This parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created the parameter cannot be modified. If you need to change the value of this parameter you must first delete the SAP and create a new one that matches the new requirements.

20 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

21 Click on the OK button. The Site (Create) form reappears.

22 Repeat steps 12 to 21 for each access interface to be created on the site.

23 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

24 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service navigation tree.

25 Click on the OK button to close the VLAN (Create) form.

Procedure 69-3 To create an L2 VPN TLS VLAN service

Perform the following procedure to create a L2-VPN (TLS/VLAN-Stacking) service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the L2 VPN TLS VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the L2 VPN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State
  This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Set the Application parameter to L2-VPN (TLS/VLAN-Stacking).

7 Click on the Select button in the Group panel to choose a group to associate with the L2 VPN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab.

11 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

12 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

13 Configure the parameters.

- Description
- Administrative State

14 Click on the Port tab button.

15 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

16 Use the configurable filter and Search button to choose a port for user-side access to the L2 VPN service, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

17 Configure the remaining parameters, if required.

18 Click on the VLAN tab button.

19 Configure the VLAN Tagging parameter. This parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created, the parameter cannot be modified. If you need to change the value of this parameter, you must first delete the SAP and then create a SAP that matches the new requirements.

20 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

21 Click on the OK button. The Site (Create) form reappears.

22 Repeat steps 12 to 21 for each access interface to be created on the site.

23 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

24 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service navigation tree.

25 Click on the OK button to close the VLAN (Create) form.

Procedure 69-4 To create an OmniSwitch L2 VPN TLS VLAN service

Note 1 — The TLS Mode must be set to Ethernet Service before a sL2 VPN TLS (stacked) VLAN service can be created on an OmniSwitch. See Procedure 31-54 to configure the TLS Mode.

Note 2 — Alcatel-Lucent recommends that you configure OmniSwitch network ports before you configure a L2 VPN TLS VLAN service.

1 Complete steps 1 to 11 in Procedure 69-3.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 On the navigation tree, right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

4 Configure the Ethernet Service Name parameter.

5 On the navigation tree, right-click on Ethernet Service and choose Create Service Access Multipoint. The Service Access MultiPoint (Create) form opens with the General tab displayed

6 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

7 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 10.

8 Click on the Select button to choose a SAP profile to associate with the service access multipoint. The Select SAP Profile - Service Access MultiPoint form opens.

9 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

10 On the navigation tree, right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Name
- Description

12 Click on the Port tab button.

13 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

14 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

15 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise go to step 19.

16 Click on the OK button. The VLAN SAP appears in the list of service access points in the service navigation tree.

17 Click on the General tab button.

18 Repeat steps 11 to 16 to add an additional VLAN service access point.

19 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

20 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

21 Click on the Customer VLANs tab button.

22 Click on the Create button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

23 Configure the parameters:

- Customer VLAN ID
- Map Type

24 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 27.

25 Click on the OK button.

26 Repeat steps 23 to 25 to add another customer VLAN.

27 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

28 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

29 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

30 Click on the OK button. The Ethernet Service (Create) form reappears.

31 Repeat steps 5 to 30 to add another service access multipoint to the Ethernet service.

32 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

33 Click on the OK button. The Site (Create) form reappears.

34 Repeat steps 3 to 33 to add another Ethernet service to the site.

35 Click on the STP tab button.

36 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

37 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

38 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

39 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

40 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

41 Click on the OK button. The DHCP Snooping General tab reappears.

42 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

43 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

44 Configure the MAC Address parameter.

45 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

46 Choose a port from the list and click on the OK button.

47 The DHCP Snooping Binding Database (Create) form reappears.

48 Configure the parameters:

- IP Address
- Lease Time

49 Click Apply to add the static entry to the table. A dialog box appears.

50 Click on the OK button.

51 Repeat steps 42 to 50 for each static entry that you need to add to the binding table.

52 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

53 Click on the OK button. A dialog box appears.

54 Click on the OK button. The VLAN (Create) form reappears.

55 Click on the OK button to close the VLAN (Create) form.

Procedure 69-5 To create a BTV VLAN service

Perform the following procedure to create a BTV VLAN service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the BTV VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the BTV VLAN and click on the OK button. The Select Customer - VLAN Services form closes and the VLAN Services (Create) form reappears with the customer information displayed in the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State
  This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Set the Application parameter to Broadcast TV (MVR/IPMV).

7 Click on the Select button in the Group panel to choose a group to associate with the BTV VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 In the IPMVLAN panel, configure the Type parameter.

10 Click on the MVR tab button.

11 Configure the parameters.

- Mode
- Query Response Time (seconds)

12 Click on the Select button in the Multicast Package panel to choose a multicast package for the BTV VLAN. The Select Multicast Package - MvrConfiguration form opens.

13 Select a multicast package and click on the OK button. The Select Multicast Package - MvrConfiguration form closes and the VLAN (Create) form reappears with the multicast package information displayed.

14 On the navigation tree, right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

15 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed on the General tab.

16 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

17 Click on the MVR tab button to configure the Mode parameter, if required.

18 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

19 Configure the parameters.

- Description
- Administrative State

20 Click on the Port tab button.

21 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

22 Use the configurable filter and Search button to choose a port for user-side access to the BTV VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

23 Configure the remaining parameters, if required.

24 Click on the VLAN tab button.

25 Configure the VLAN Tagging parameter.

You can only configure this parameter after you create a SAP. After the SAP is created, the VLAN Tagging parameter cannot be modified. If you need to change the value of the parameter, you must first delete the SAP and then create a SAP that matches the new requirements.

26 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

27 Click on the OK button. The Site (Create) form reappears.

28 Repeat steps 18 to 27 for each access interface to be created on the site.

29 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

30 Click on the OK button. The VLAN (Create) form reappears with the site information displayed in the service navigation tree.

31 Click on the OK button to close the VLAN (Create) form.

Procedure 69-6 To create an OmniSwitch BTV VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN Service form opens.

3 Choose a customer for the VLAN and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN Service (Create) form reappears with the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State
  This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Set the Application parameter to Broadcast TV (MVR/IPMV).

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Choose a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form opens with the group information displayed.

9 In the IPMVLAN panel, configure the Type parameter.

10 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

11 Choose a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab displayed.

12 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

13 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed. The VLAN access interface serves as a receiver port on the IP multicast VLAN.

14 Configure the Description parameter.

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

17 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

Note — To configure an access interface, a L2 VPN TLS VLAN user port must be created. See Procedure 69-4.

18 Click on the VLAN tab button.

19 Configure the VLAN Tagging parameter.

20 Click on the Apply button if you need to add another VLAN access interface and the VLAN access interface appears in the list of access interfaces in the navigation tree. A dialog box appears. Otherwise, go to step 24.

21 Click on the OK button.

22 Click on the General tab button.

23 Repeat steps 14 to 21 for each additional VLAN access interface to be added to the site.

24 Click on the OK button. A dialog box appears.

25 Click on the OK button. The VLAN Access Interface (Create) form closes.

26 Right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

27 Configure the Ethernet Service Name parameter.

28 On the navigation tree, right-click on Ethernet Service and choose Create Service Access MultiPoint. The Service Access MultiPoint (Create) form opens with the General tab displayed.

29 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

30 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 33.

31 Click on the Select button to choose a SAP profile to associate with the service access multi-point. The Select SAP Profile - Service Access MultiPoint form opens.

32 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

33 On the navigation tree, right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

34 Configure the parameters:

- Name
- Description

35 Click on the Port tab button.

36 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrids. After you do this, the port is listed when you click on the Search button.

37 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

38 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise, go to step 42.

39 Click on the OK button. The VLAN service access point appears in the list of Service Access Points on the service navigation tree.

40 Click on the General tab button.

41 Repeat steps 33 to 39 to add an additional VLAN SAP.

42 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

43 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

44 Click on the Customer VLANs tab button.

45 Click on the Create button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

46 Configure the parameters:

- Customer VLAN ID
- Map Type

47 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 50.

48 Click on the OK button.

49 Repeat steps 46 to 48 to add another customer VLAN.

50 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

51 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

52 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

53 Click on the OK button. The Ethernet Service (Create) form reappears.

54 Repeat steps 28 to 53 if you need to add another service access multipoint to the Ethernet service.

55 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

56 Click on the OK button. The Site (Create) form reappears.

57 Repeat steps 26 to 56 if you need to add another Ethernet service to the site.

58 Click on the STP tab button.

59 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

60 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

61 Click on the Create button. The VLAN Level DHCP Snooping (Create) form opens.

62 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

63 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

64 Click on the OK button. The DHCP Snooping General tab reappears.

65 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

66 Click on the Create button. The DHCP Snooping Binding Database (Create) form opens.

67 Configure the MAC Address parameter.

68 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

69 Choose a port from the list and click on the OK button.

70 The DHCP Snooping Binding Database (Create) form reappears.

71 Configure the parameters:

- IP Address
- Lease Time

72 Click Apply to add the static entry to the table. A dialog box appears.

73 Click on the OK button.

74 Repeat steps 65 to 73 for each static entry that you need to add to the binding table.

75 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

76 Click on the Multicast Groups tab button.

77 Click on the Create button to add a multicast group address to the site. The Multicast Group (Create) form opens.

78 Configure the Multicast Address parameter.

79 Click on the Apply button if you need to add another multicast address. A dialog box appears. Otherwise, go to step 82.

80 Click on the OK button. The multicast address information appears on the Site (Create) form.

81 Repeat steps 78 to 80 to add another multicast address to the site.

82 Click on the OK button.

83 Click on the Customer VLAN Tags tab button.

84 Click on the Create button to add a customer VLAN tag to the site. The Customer VLAN Tag (Create) form opens.

85 Configure the Customer VLAN Tag parameter.

86 Click on the Apply button if you need to add another customer VLAN tag. The customer VLAN tag information appears on the Site (Create) form. A dialog box appears. Otherwise, go to step 89.

87 Click on the OK button.

88 Repeat steps 85 to 87 to add another customer VLAN tag to the site.

89 Click on the OK button.

90 Click on the OK button to the close the Site (Create) form. A dialog box appears.

91 Click on the OK button. The Site (Create) form closes.

92 Click on the OK button to close the VLAN (Create) form.

Procedure 69-7 To create a super VLAN service

Perform the following procedure to create a super VLAN (Internet Access) service on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the super VLAN. The Select Customer - VLAN Service form opens.

3 Select a customer for the super VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State

This parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

5 Click on the VLAN tab button.

6 Configure the Application parameter. Choose the Internet Access (Super-VLAN) option.

7 Click on the Select button in the Group panel to choose a group to associate with the super VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

10 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form reappears with the site information displayed on the General tab.

11 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

12 On the navigation tree, right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

13 Configure the parameters.

- Description
- Administrative State

14 Click on the Port tab button.

15 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

16 Use the configurable filter and Search button to choose a port for user-side access to the super VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

17 Configure the remaining parameters, if required.

18 Click on the VLAN tab button.

19 Configure the parameter.

- VLAN Tagging

You can only configure this parameter when you create a SAP. After the SAP is created the parameter cannot be modified. If you need to change the value of this parameter you must first delete the SAP and create a new one that matches the new requirements.

The VLAN Tagging parameter should always be set to Tagged on CES interfaces.

20 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

21 Click on the OK button. The Site (Create) form reappears.

22 Repeat steps 12 to 21 for each access interface to be created on the site.

23 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

24 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service navigation tree.

25 Click on the OK button to close the VLAN (Create) form.

Procedure 69-8 To create a 9500 MPR (dot1q) VLAN service

Before you create a 9500 MPR (dot1q) VLAN service, perform the following procedures:

- Create a customer profile. See Procedure 67-1.
- Create a VLAN group. See Procedure 69-10.
- Create a VLAN path if you need to assign a specific VLAN path to the 9500 MPR (dot1q) VLAN service. See Procedure 69-12.

1 Right-click on a 9500 MPR in the navigation tree and choose Properties from the contextual menu. The 9500 MPR properties form opens with with the General tab displayed.

2 Click on the System Settings tab and set the Bridge Type parameter to 802.1Q.

3 Close the 9500 MPR properties form.

4 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) Service form opens with the General tab displayed.

5 Click on the Select button to choose a customer to associate with the 9500 (dot1q) VLAN service. The Select Customer - VLAN Service form opens.

6 Choose a customer for the 9500 MPR (dot1q) VLAN service and click on the OK button. The Select Customer - VLAN Service form closes and the VLAN (Create) Service form reappears with the customer information displayed on the General tab.

7 Configure the parameters:

- Service ID
  The Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  The SVC Mgr Service ID parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- OLC State
  The OLC State parameter is configurable when you click on the Apply button on the VLAN Service (Create) form.

8 Click on the VLAN tab button and set the Application parameter to 9500 VLAN.

9 Click on the Select button in the Group panel to choose a VLAN group to associate with the 9500 MPR (dot1q) VLAN service. The Select Group - VLAN Service form opens.

10 Select a VLAN group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

11 Perform one of the following:

a Enable the Auto-Assign ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

b Disable the Auto-Assign ID parameter to configure the VLAN ID parameter.

12 Perform one of the following:

a Enable the Specify VLAN Path parameter.

b Disable the Specify VLAN Path parameter to specify a VLAN path by clicking on the Select button in the VLAN path panel. Go to step 16.

13 Configure the parameters:

- Path Type
- Point to Point VLAN
  The Point to Point VLAN parameter is configurable when the Path Type parameter is set to Hop Based.

Note — The service created using Point to Point VLAN service will be discovered as a normal VLAN service without the point-to-point option.

14 Click on the Select button in the VLAN Path panel to choose a VLAN Path to associate with the 9500 MPR (dot1q) VLAN service. The Select VLAN Path - VLAN Service form opens.

15 Choose a VLAN Path and click on the OK button. The Select VLAN Path - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

Note 1 — The VLAN path may consist of consecutive physical links, non-consecutive physical links, or radio links spanning NEs.

Note 2 — You cannot reconfigure the Point to Point VLAN parameter after you choose a VLAN path. To change the parameter, you are required to clear the selected VLAN path.

16 On the navigation tree, right-click on VLAN and choose Create VLAN Site. The Select Network Elements - VLAN form opens.

Note — The service navigation tree will be auto-populated with sites that correspond to the hops in the specified VLAN Path.

17 Choose a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab.

18 Configure the parameters:

- Description
- Administrative State
- Monitor Access Interface Operational State

19 Click on the OK button. The Site (Create) form closes and a dialog box appears.

20 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service navigation tree.

21 Click on the OK button to close the VLAN (Create) form.

Procedure 69-9 To associate an access interface with a VLAN service

Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service to be associated with an interface, and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 On the navigation tree, click on the site to which you want to associate the new access interface; expand the entries for that site.

4 Right-click on the Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

5 Configure the parameters.

- Description
- Administrative State

6 Click on the Port tab button.

7 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

8 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

9 Configure the remaining parameters, if required.

10 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

11 Click on the OK button. The VLAN - *Service Name* (Edit) form reappears with the new interface displayed in the service navigation tree under Access Interfaces for the site specified in step 3.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button to confirm the action and close the dialog box. The Manage Services form reappears.

14 Click on the Close button to close the Manage Services form.

Procedure 69-10 To create a VLAN group

1 Choose Manage→VLAN→VLAN Groups from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Click on the Create button. The VLAN Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Node Type
- Technology
- Topology
- VLAN Space Management by SAM
- Head Ends

You can configure the VLAN Space Management by SAM parameter when the Node Type parameter is set to 9500.

You can configure the Head Ends parameter when the Node Type parameter is set to OMNI.

4 Click on the Apply button.

5 Click on the Group Members tab button.

6 Click on the Create button. The Select Network Elements form opens and a list of available NEs is displayed. Only NE types specified by the Node Type parameter are displayed in the list.

7 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

8 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

9 If you enabled the Head Ends parameter, you can add head end NEs to the group. Otherwise, go to step 13.

10 Click on the Add Headend Node button. The Select Network Elements form opens and a list of available NEs is displayed. Only 7750 SR, 7710 SR, and 7450 ESS NE types are displayed in the list.

11 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

12 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

13 If you need to apply a span of control to a group, other than the default, click on the Spans tab button. Otherwise, go to step 14.

  i Click on the Create button. The Select Span(s) - VLAN Group form opens with a list of available spans.

  ii Choose one or more spans of control to apply to the VLAN group.

  iii Click on the OK button. The Select Span(s) - VLAN Group form closes and a dialog box appears.

  iv Click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VLAN Group (Edit) form closes.

16 A list of VLAN groups is displayed in the Manage VLAN Groups form.

17 Close the Manage VLAN Groups form.

Procedure 69-11 To delete a VLAN group or group member

Note 1 — You must delete all of the members from a group before you can delete the group.

Note 2 — A 9500 MPR group member cannot be deleted if it is part of a VLAN path.

1 Choose Manage→ VLAN→VLAN Group from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Apply a filter, or create and apply a filter, and click on the Search button. A list of VLAN groups is displayed.

3 Choose a VLAN group from the list.

4 Click on the Properties button. The VLAN Group (Edit) form opens with the General tab displayed.

5 Click on the Group Members tab button.

6 If the group does not contain any members, go to step 9. Otherwise go to step 7.

7 Choose one or more members of the VLAN group and click on the Delete button. A dialog box appears.

8 Click on the OK button to delete the group members.

9 Close the VLAN Group (Edit) form. The Manage VLAN Groups form is displayed.

10 Choose the VLAN group that you need to delete from the displayed list.

11 Click on the Delete button. A dialog box appears.

12 Click on the Yes button to delete the VLAN group.

13 Close the Manage VLAN Groups form.

Procedure 69-12 To create a 9500 MPR VLAN path

Note 1 — When you create an Auto or Point 2 Point variant of a hop-based VLAN path, all of the 9500 MPR NEs that traverse the VLAN path must be part of the same VLAN group. For Manual VLAN paths variants, a VLAN group is not required. See Procedure 69-10 for information about creating VLAN groups.

Note 2 — To create a ring-based VLAN path, you need a radio ring element. See Procedure 33-9 for information about creating a radio ring element.

1 Choose Manage→VLAN→Paths from the 5620 SAM main menu. The Manage VLAN Paths form opens.

2 Click on the Create button. The Create VLAN Path form opens with the Path Type step displayed.

3 Configure the Path Type parameter.

4 Click on the Next button. The Identification step is displayed.

5 Configure the parameters:

- Name
- Description
- Creation Type

  The Creation Type parameter appears when the Path Type parameter is set to Hop Based.

6 Click on the Next button. For ring based VLAN paths, the Select Ring step is displayed. For hop-based VLAN paths, the Specify Vlan Path Constraints step is displayed.

7 Perform one of the following:

a If you configured the Ring Based option for the Path Type parameter, go to step 8.

b If you configure the Hop Based option for the Path Type parameter, go to step 10.

8 Click on the Select button. The Select Ring - VLAN Path opens.

9 Choose a radio ring in the list and click on the OK button. The Select Ring - VLAN Path form closes and the address of the selected Radio Ring is displayed in the Mgr ID parameter. Go to Step 41.

10 Perform one of the following:

a If you configured the Manual option for the Creation Type parameter, go to step 11.

b If you configured the Auto or Point 2 Point options for the Creation Type parameter, go to step 22.

11 Configure the Minimum Bandwidth (kbps) parameter.

12 Click on the Next button. The Define Source Site step is displayed.

13 Perform one of the following:

a Enter the IP address of the starting VLAN path endpoint in the Starting Network Element parameter.

b Click on the Select button. The Select a Network Element - Define Source Site form opens. Choose a 9500 MPR in the list and click on the OK button. The Select a Network Element - Define Source Site form closes and the IP address of the selected 9500 MPR is displayed in the Starting Network Element parameter.

14 Click on the Next button. The Define the Provisioned Path step is displayed

15 Click on the Insert Hop button to insert a VLAN path hop. The Hop for New VLAN Path (Create) form opens.

16 Click on the Select Network Element button. The Select a Network Element - New VLAN Path form opens.

17 Choose a 9500 MPR in the list and click on the OK button. The New VLAN Path form closes and the IP address of the NE is displayed in the Network Element parameter.

18 Click on the Select Link button. The Select Links - New VLAN Path form opens.

19 Choose a link from the list and click on the OK button.

20 Click on the Apply button if you need to add another hop. Click on the OK button after you add all of the required hops.

21 Close the Hop for New VLAN Path (Create) form. Go to Step 41.

22 Configure the parameters:

- Max Hops
- Minimum Bandwidth (kbps)
- Select Shortest Path

23 Perform one of the following:

a If you selected the Auto option for the Creation Type parameter in Step 5, go to Step 24.

b If you selected the Point 2 Point option for the Creation Type parameter in Step 5, go to Step 31.

24 Click on the Next button. The Define Head step is displayed.

25 Perform one of the following:

a In the Head End parameter, enter the IP address of the 9500 MPR at the head end of a VLAN group.

b Click on the Select button. The Select a Network Element - Define Head End form opens. Choose a 9500 MPR in the list and click on the OK button. The Select a Network Element - Define Head End form closes and the IP address of the selected 9500 MPR is displayed in the Head End parameter.

26 Click on the Next button. The Possible Vlan Path step is displayed.

27 Click on the Insert Hop button to insert a VLAN path hop. The Hop (Create) form opens.

28 Choose a 9500 MPR in the list and click on the OK button. The New VLAN Path form closes and the IP address of the NE is displayed in the Network Element parameter.

29 Click on the Apply button if you need to add an additional hop. Click on the OK button after you add all of the hops.

30 Close the Hop (Create) form. Go to Step 41.

31 Click on the Next button. The Define Source Site step is displayed.

32 Perform one of the following:

- **a** Enter the IP address of the starting VLAN path endpoint in the Starting Network Element parameter.
- **b** Click on the Select button. The Select a Network Element - Define Source Site form opens. Choose a 9500 MPR in the list and click on the OK button. The Select a Network Element - Define Source Site form closes and the IP address of the selected 9500 MPR is displayed in the Starting Network Element parameter.

33 Click on the Next button. The Define Destination Site step is displayed.

34 Perform one of the following:

- **a** Enter the IP address of the destination VLAN path endpoint in the Destination Network Element parameter.
- **b** Click on the Select button. The Select a Network Element - Define Destination Site form opens. Choose a 9500 MPR in the list and click on the OK button. The Select a Network Element - Define Destination Site form closes and the IP address of the selected 9500 MPR is displayed in the Destination Network Element parameter.

35 Click on the Next button. The Possible VLAN Path step is displayed.

36 Click on the Insert Hop button to insert a VLAN path hop. The Hop for New VLAN Path (Create) form opens.

37 Click on the Select Network Element button. The Select a Network Element - New VLAN Path form opens.

38 Choose a 9500 MPR in the list and click on the OK button. The New VLAN Path form closes and the IP address of the NE is displayed in the Network Element parameter.

39 Click on the Apply button if you need to add an additional hop. Click on the OK button after you add all of the hops.

40 Close the Hop for New VLAN Path (Create) form.

41 Click on the Finish Button to save the VLAN path configuration.

42 Click on the Close button. The Create VLAN Path form closes.

43 Close the Manage VLAN Paths form.

Procedure 69-13 To delete a 9500 MPR VLAN path

Note — You cannot delete a VLAN path if the path is being used by a service.

1 Choose Manage→VLAN→Paths from the 5620 SAM main menu. The Manage VLAN Paths form opens.

2 Apply a filter, or create and apply a filter, and click on the Search button. A list of VLAN paths is displayed.

Note — If VLAN paths are already in your network, the 9500 MPR NE that the path traverses is auto-discovered by the 5620 SAM. The paths appear on the Manage VLAN Paths form with a name with the following syntax: *Discovered-VLANPath-<IP address of the source 9500 MPR>-<IP address of the destination 9500 MPR*

3 Choose a VLAN path from the list and click on the Delete button. The VLAN path and all of the associated hops are deleted.

4 Close the Manage VLAN Paths form.

Procedure 69-14 To add a MEP to an OmniSwitch VLAN service access interface

Perform the procedure to manually add a MEP to an OmniSwitch VLAN service access interface. See Chapter 80 for more information on MEPs.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 On the navigation tree, click on the site to which you want to add the MEP; expand the entries for that site.

4 Right-click on the access interface and click on Properties. The VLAN Access Interface (Edit) form opens with the General tab displayed.

5 Click on the MEPs tab button.

6 Click on the Create button.

7 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

8 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

9 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect

10 Click on the OK button. The VLAN Access Interface (Edit) form reappears.

11 Click on the Refresh button to update the MEP list.

12 Repeat steps 6 to 11 to add additional MEPs.

13 Close the VLAN Access Interface (Edit) form to return to the VLAN Service (Edit) form.

14 Close the VLAN Service (Edit) form.

15 Close the Manage Services form.

Procedure 69-15 To configure IGMP on an OmniSwitch VLAN site

OmniSwitch IGMP parameters can be configured globally and per VLAN site. You can configure VLAN site IGMP parameters only after you create the VLAN. VLAN IGMP configuration settings override global IGMP settings. See Procedure 31-38 for information about configuring global OmniSwitch IGMP parameters.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an OmniSwitch VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab button.

6 Choose a site from the list and click on the Properties button. The Site (Edit) form opens with the General tab displayed.

7 Click on the IGMP tab button.

8 Choose an entry from the list and click on the Properties button. The IGMP (Edit) form opens with the General tab displayed.

9 Configure the following parameters, if required:

- Administrative State
- Querying
- Spoofing
- Proxying
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Querier Forwarding
- Zapping
- Max Group Action
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)

10 Click on the Multicast Group tab button to create a static IGMP group.

11 Click on the Create button. The Group (Create) form opens.

12 Click on the Select button to choose a terminating port. The Select Port - Group form opens with a list of available ports.

13 Choose a port from the list and click on the OK button. The Select Port - Group form closes and the selected port is displayed on the Group (Create) form.

14 Configure the Multicast Group IP Address parameter.

15 Click on the OK button. The Select Port - Group form closes, the multicast group appears in the listing, and a dialog box appears.

16 Click on the OK button.

17 Repeat steps 11 to 16 for each multicast group that you need to add.

18 Click on the Multicast Neighbor tab button to create a static IGMP neighbor.

19 Click on the Create button. The Neighbor (Create) form opens.

20 Click on the Select button to choose a terminating port. The Select Port - Neighbor form opens with a list of available ports.

21 Choose a port from the list and click on the OK button. The Select Port - Neighbor form closes and the selected port is displayed on the Neighbor (Create) form.

22 Click on the OK button. The Select Port - Neighbor form closes, the multicast neighbor appears in the listing, and a dialog box appears.

23 Click on the OK button.

24 Repeat steps 19 to 23 for each multicast neighbor that you need to add.

25 Click on the Multicast Querier tab button to create a static IGMP querier.

26 Click on the Create button. The Querier (Create) form opens.

27 Click on the Select button to choose a terminating port. The Select Port - Querier form opens with a list of available ports.

28 Choose a port from the list and click on the OK button. The Select Port - Querier form closes and the selected port is displayed on the Querier (Create) form.

29 Click on the OK button. The Select Port - Querier form closes, the multicast querier appears in the listing, and a dialog box appears.

30 Click on the OK button.

31 Repeat steps 26 to 30 for each multicast querier that you need to add.

32 Click on the OK button to close the IGMP (Edit) form.

33 Click on the OK button to close the Site (Edit) form

34 Click on the OK button to close the VLAN (Edit) form

35 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

36 Click on the Close button to close the Manage Services form.

Procedure 69-16 To run an OAM validation test on a VLAN service

A validator test suite must be created for the tested entity. See chapter 78 for more information about how to create a validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens with the General tab displayed.

4 Click on the More Actions button and choose Validate. If a validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

  i Click on the OK button to associate the service with an existing validator test suite. The Choose Validator Test Suite form appears.

  ii Configure the filter criteria. A list of validator test suites appears.

  iii Select a validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the VLAN (Edit) form.

11 Close the Manage Services form.

Procedure 69-17 To view the VLAN service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VLAN (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 69-18 To view the service topology associated with a VLAN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 5 for more information about service topology views.

Procedure 69-19 To modify a VLAN service

Caution — Modifying parameters can be service-affecting.

Note — Restrictions apply to VLANs using 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices. See "7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, 7210 SAS-M and Telco VLAN restrictions" in this chapter, for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs contain non-configurable parameter information for the service:

- VLAN tab—displays information about the VLAN type
- MVR tab—displays multicast package policy information for the service

The MVR tab button is not selectable for some types of VLAN.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Sites tab—lists the sites that are included in the service
- VLAN Access Interfaces tab—lists the L2 access interfaces that are included in the service
- Ethernet Services—lists the Ethernet services
- Service Termination Point tab — lists the ports on the far end points of the service
- Template tab — displays the template used to create the mirror service, if applicable.
- Faults tab—displays the faults associated with the service

The Ethernet Services tab button is not selectable for some types of VLAN.

Note — Users with the administrator scope of command role can click on the Select button on the Templates tab to associate a service template with the service object, if required.

5 Modify the parameters for the service as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

8 Click on the Close button to close the Manage Services form.

Procedure 69-20 To delete a VLAN service

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

Caution — Do not delete any VLANs that are used for network management, otherwise connectivity between the 5620 SAM and the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, OmniSwitch, or Telco devices is lost.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This message is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

70 — VLL service management

70.1 VLL service management overview

The 5620 SAM supports the provisioning of VLL services on edge devices. A VLL service is an L2 point-to-point service that connects access interfaces. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this, the device performs no MAC learning in a VLL service.

The 5620 SAM supports multiple variations of VLL services. See “VLL types” in this section for more information.

A VLL service that connects access interfaces on one device is called a local VLL service. As there is no need for signaling between devices, a local VLL service uses no SDPs.

A VLL service that connects access interfaces on two devices is called a distributed VLL service. Subscriber or customer data enters a distributed VLL service through access interfaces on different edge devices. The VLL service encapsulates the data and transports it across a service provider IP/MPLS network through GRE or MPLS service tunnels.

Packets that arrive at an edge device are associated with a VLL service based on the access interface on which they arrive. An access interface is uniquely identified using these parameters:

- physical port or POS port and channel
- encapsulation type
- encapsulation identifier (if required, depending on encapsulation type)

A VLL service uses T-LDP signaling, and uses MPLS or GRE as the service tunnel transport.

A new or existing VLL can be configured as the spoke of an HVPLS. See “HVPLS” in section 71.1 and chapter 76 for more information.

The 5620 SAM supports end-to-end VLL configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the template management role can create a service template. The template management user can also configure and bind site, circuit, and L2 interface templates to the service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

Common to all device services, such as VLL, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form. Because a VLL service is a point-to-point service, ingress QoS policies create only the unicast queues that are defined in the policy and not the multicast queues.
- (Epipe service only) Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and changes to the current access line rate between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 46 for more information about policies.

OAM diagnostics can be performed on a per-service basis. See chapter 38 for more information.

The General tab of the VLL service management form displays information about the operational state of the service and its sites through the Operational State and State Cause indicators.

The Operational State indicator identifies the states of the sites that are part of the service, as follows:

- Up—one operational path in both directions (end-to-end)
- Down—path is not operationally complete

When the Operational State is Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

You can run the OAM Validation test suite for the service by clicking on the More Actions > Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 78 for more information about how to configure OAM validation test suites.

The 5620 SAM also monitors the status of a peer SAP after a VLL has been created and put into service. Status information includes faults detected on the service tunnel, and access and network SAP transmissions and receptions. The States tab of the Spoke SDP Binding form displays indicators of failure in the VLL in the State Cause panel.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 76 for more information about the hierarchical organization of composite services.

VLL types

The 5620 SAM supports the creation of the following VLL service types:

- Epipe, or Ethernet VLL service
- Apipe, or ATM VLL service
- Fpipe, or frame relay VLL service
- Hpipe, or HDLC service
- Ipipe, or IP interworking VLL service
- Cpipe, or circuit emulation VLL service

Epipe (Ethernet VLL)

An Epipe, or Ethernet VLL service, provides a point-to-point Ethernet service. One endpoint of an Epipe uses Ethernet encapsulation, and the other endpoint uses Ethernet, ATM, frame relay encapsulation, or CEM encapsulation. An Epipe effectively provides ATM and frame relay bridged encapsulation termination for interworking. The 5620 SAM supports local cross-connecting when the Epipe endpoints are on the same device. The device supports these Epipe connectivity scenarios:

- a frame relay or ATM user in an ATM network communicating with an Ethernet user on an IP/MPLS network
- a frame relay or ATM user who connects to a PE device in an IP/MPLS network and communicates with an Ethernet user who connects to another PE device in the same network

ATM users connect through a UNI using AAL-5 or bridged Ethernet PDUs, and use the VCI/VPI as the ATM SAP identifier. Frame relay users connect through a UNI that uses Multiprotocol Interconnect over frame relay or bridged Ethernet PDUs, or over an Ethernet UNI interface. The DLCI is the frame relay SAP identifier. The VCI/VPI and DLCI identifier tags are transparent to the service and remain unaffected during transport.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Epipe service:

- null
- dot1q
- SONET/SDH BCP-null
- SONET/SDH BCP-dot1q

Epipe services allow you to designate a dot1q encapsulated SAP as the default SAP for a specific port. For more information about how you can use default SAPs on an Ethernet port, see "Default SAPs" in section 71.1.

A default SAP can co-exist with other SAPs on a port, but it cannot be implemented on a null encapsulated port. Through the SAM 5620 interface, you can create a default SAP by specifying an outer encapsulation value of 4095 or * to a SAP. If OSSI is used, the outer encapsulation value is always 4095.

Apipe (ATM VLL)

An Apipe, or ATM VLL service, provides a point-to-point ATM service between users who connect to 7750 SR, 7710 SR, 7705 SAR, or 7450 ESS NEs in an IP/MPLS network directly or through an ATM access network. One endpoint of an Apipe uses ATM encapsulation and the other endpoint uses ATM or frame relay encapsulation. An ATM PVC—for example, a VC or a VP—is configured on the managed device. As a result, the ATM switches at the service endpoints appear to be directly connected over an ATM link. The 5620 SAM supports VPI/VCI translation in an Apipe and supports local cross-connecting when the Apipe endpoints are on the same managed device.

An Apipe encapsulates standard UNI/NNI cells that ingress the ATM SAP into a pseudowire packet using N:1 cell mode encapsulation or AAL-5 SDU mode encapsulation. When using N:1 cell mode encapsulation, an Apipe supports cell concatenation into a pseudowire packet and the setup of both VC- and VP-level connections.

For ATM and frame relay interworking, an Apipe provides a point-to-point service between a user who connects to an existing ATM network and another user who connects to a PE in an IP/MPLS network. An ATM AAL-5 SDU pseudowire or a frame relay 1-to-1 mode pseudowire connects the nodes. The PE performs an FRF.5 interworking function to join the ingress and egress data paths.

An ATM VT SAP on a PE is identified by the physical port and VPI range. Cells that arrive on a specified port and are within the specified VPI range go into a single pseudowire for transport through the IP/MPLS network. A user can configure the whole ATM port as a VT and does not need to specify a VPI range. There is no ingress or egress VPI/VCI translation or loss of cell order.

The 7705 SAR uses N>1 cell mode encapsulation to support multiple VCs on an Apipe. You can multiplex VCs on a 7705 SAR Apipe service using SAP aggregation groups. See Procedure 70-14 for more information on configuring SAP aggregation groups.

The 5620 SAM supports the ATM N:1-N>1 VC type to allow interoperability between 7705 SAR and 7750 SR Apipe services, despite each site using different cell mode encapsulation. An interoperating Apipe service uses the ATM N:1-N>1 VC type, while the 7705 SAR site uses ATM VCC and the 7750 SR uses ATM Cell. An interoperating Apipe service combines SAP aggregation groups from the 7705 SAR Apipe with connection profiles from the 7750 SR Apipe onto a single Apipe service.

Fpipe (frame relay VLL)

An Fpipe, or frame relay VLL service, provides a point-to-point frame relay service between users who connect to PE 7750 SR, 7710 SR, or 7450 ESS NEs in an IP/MPLS network. Both endpoints of an Fpipe use frame relay encapsulation. An Fpipe connects users through frame relay PVCs. An Fpipe receives standard Q.922 core frames on the frame relay SAP and encapsulates them in a pseudowire packet according to the 1-to-1 frame relay encapsulation mode. This is the VC type used on the SDP by default. The 5620 SAM does not support the many-to-one, or port encapsulation, mode. Fpipe creation supports local cross-connecting when the endpoints are on the same managed device.

Hpipe (HDLC VLL)

An Hpipe, or HDLC VLL service, is used to carry HDLC PDUs over an MPLS network. HDLC PWs enable service providers to offer emulated HDLC services over existing MPLS networks. HDLC mode provides port-to-port transport of HDLC-encapsulated traffic.The HDLC PDU is transported in its entirety, including the HDLC address and control fields, but the HDLC flags and the FCS are excluded. If the optional control word is used, the flag bits in the control word are not used and must be set to 0 for transmitting and must be ignored upon receipt.

Before HDLC SAPs can be configured, the mda-mode command must be set to cem-fr-hdlc-ppp at the card level. Only ports that are configured with HDLC encapsulation can be mapped to an Hpipe SAP.HDLC encapsulating ports do not terminate the HDLC. The ports pass the HDLC frames through the Hpipe. HDLC encapsulated ports can pass through any HDLC-framed traffic, such as Cisco-HDLC, FR, PPP, etc.

Ipipe (IP interworking VLL)

An Ipipe, or IP interworking VLL service, uses the IP/MPLS network to provide Layer 3 connectivity between different Layer 2 technologies. An Ipipe service provides point-to-point IP connectivity between a user on a frame relay, ATM, cHDLC, or PPP access circuit with routed PDU IPv4 encapsulation and a user on an Ethernet interface. The Ethernet SAP interface can terminate on a 7705 SAR, 7750 SR, 7450 ESS, or 7710 SR.

Table 70-1 summarizes the supported SAP types.

Table 70-1 Supported SAP types

SAP Types	Frame relay	ATM	PPP/IPCP	cHDLC	Ethernet
Frame relay	✓	✓			✓

(1 of 2)

SAP Types	Frame relay	ATM	PPP/IPCP	cHDLC	Ethernet
ATM	✓	✓			✓
PPP/IPCP			✓		✓
cHDLC				✓	✓
Ethernet	✓	✓	✓	✓	✓

(2 of 2)

In an Ipipe service, both CE devices appear to be on the same IP interface. The PE devices must therefore resolve Layer 2 addresses when different resolution protocols are used on either SAP. Each PE device is manually configured with the IP addresses of both CE devices, or alternatively, can be set to automatically discover the IP addresses of the CE routers. The PE device maintains an ARP cache context for each IP interworking VLL, and responds to ARP request messages received on the Ethernet SAP. The PE device responds with the Ethernet SAP configured MAC address as a proxy for an ARP request for the frame relay, ATM, or PPP user access circuit IP address, and silently discards any ARP request message received on the Ethernet SAP for any other address. The PE device maintains a record of the association of IP addresses with MAC addresses for ARP requests that it receives over the Ethernet SAP.

An Ipipe SAP can be bound to a physical or logical port with PPP, cHDLC, ATM, or FR encapsulation. On Release 8.0 R5 or earlier NEs, when IPv6 is enabled, cHDLC, ATM and FR encapsulation are not supported. ATM users connect through a UNI using AAL-5 MUX IP or AAL-5 SNAP routed PDU encapsulation. Frame relay users connect using routed PDU IPv4 encapsulation. PPP interfaces use PPP/IPCP encapsulation of an IPv4 packet. Users of cHDLC connect using routed IPv4 encapsulation.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Ipipe service:

- Null
- dot1q
- Q in Q

Note — IPCP SAPs on the 7705 SAR can be configured to assign primary and secondary DNS addresses to the remote peer.

The following identifiers are used for packet forwarding:

- VCI/VPI as the ATM SAP identifier
- DLCI as the frame relay SAP identifier

Cpipe (circuit emulation VLL)

A Cpipe, or circuit emulation VLL service, provides a point-to-point CEM service between users who connect directly to 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7705 SAR, 7710 SR, or 7750 SR devices, or to 7450 ESS devices in an IP/MPLS network. The endpoints of a Cpipe use CEM encapsulation.

Note — The creation of point-to-point Cpipe CEM services on a 7450 ESS is supported only on a Release 8.0 R5 or later 7450 ESS.

The Cpipe L2 access interface can be bound to a unstructured DS1 or E1 channel, a channelized DS0 channel group, or a DS0 group with CAS signalling. Consider the following when creating a Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints.
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

VLL spoke switching

VLL spoke switching allows you to create a VLL service by cross-connecting two spoke SDPs. Spoke switching allows you to scale L2 services, such as VLLs and H-VPLS, over a multi-area network without the requirement for a full mesh T-LDP. The 5620 SAM supports spoke switching on all VLL types, however, all service instances must be the same type.

The 5620 SAM supports VLL services with spoke switching on the 7750 SR and 7450 ESS.

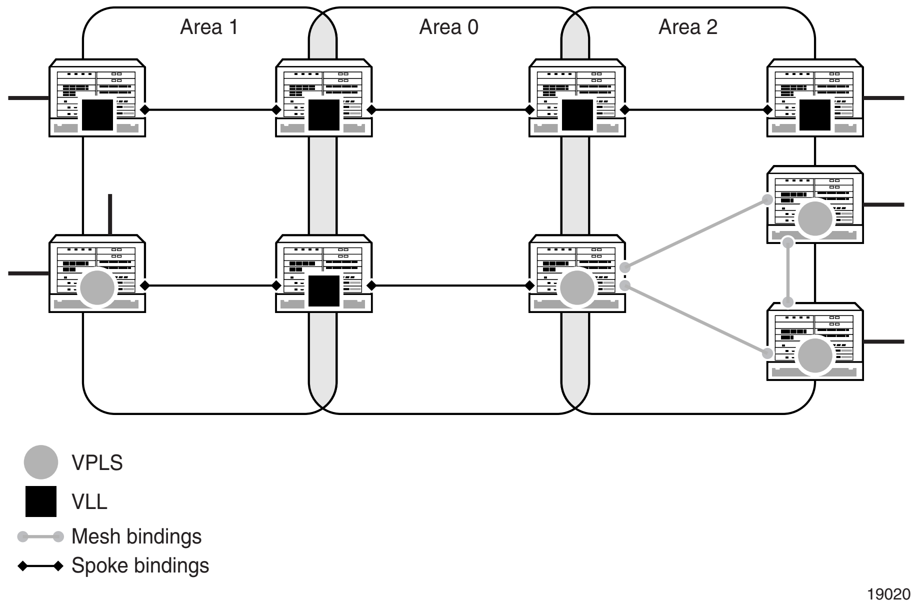
Table 70-2 describes the VLL site types that you can use in a spoke switching configuration.

Table 70-2 VLL site types

VLL site type	Description
Terminating	VLL instance has one or two VLL SAPs.
Switching	VLL instance cross-connects two spoke bindings.

Figure 70-1 shows a switching VLL that connects two VPLS. The configuration uses two T-PEs, three S-PEs, and two pairs of spoke bindings to connect the two VPLS.

Figure 70-1 VLL spoke switching



Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching:

- Service type must be a VLL at the switching node.
- VC IDs can be different for the segments in the service.
- Segments in the service can run on different types of tunnels; for example, LDP, GRE, and RSVP SDPs.
- VLL instances in a service must use the same service ID to avoid the discovery of multiple and composite services.
- VLL with one or more switching sites must have two or more terminating sites.
- Autobinding creation service is not supported for switching VLLs.

VLL redundancy

VLL redundancy requires that you associate the SAP or SDP bindings to an endpoint. You can configure the endpoint association as active or standby so that you can create a redundant configuration. The associated nodes use signaling to determine the active SAP or SDP binding. The 5620 SAM supports VLL redundancy on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

A VLL service site can have up to two local endpoints. A local endpoint combines a SAP with a binding (access) or a group of bindings (network). A SAP or an SDP binding can also exist without an endpoint association.

The 7450 ESS, 7710 SR, and 7750 SR support HSDPA offload fallback for VLL Apipe and Epipe services by allowing fallback from an active PW on a primary spoke SDP to a secondary SAP.

Table 70-3 describes the components in redundant VLL configurations.

Table 70-3 VLL components for redundant configurations

VLL component	Description
Primary or Redundant binding	Primary or redundant binding is the same as a regular spoke binding. Up to four spoke bindings can form a VLL instance network endpoint. Only one binding can be configured as the primary; up to 3 others can only be configured as redundant spokes. Each redundant spoke has a precedence value to decide which spoke is the immediate backup. Only the terminating VLL instance can have multiple bindings on the network side endpoint. A switching VLL instance has up to 2 bindings, one on each side.
Inter-Chassis Backup	You can use an ICB in conjunction with a redundant SAP to provide protection for the SAP. The SAP must also be associated with a MC-LAG or MC-APS port. The ICB transports network traffic to the SAP on the second PE when the local SAP is unavailable. You must define a switching state for the redundant SAP. You must also configure the return ICB on the opposite endpoint of the protected site.

Configuration options

Table 70-4 describes the redundancy configuration options for each VLL site.

Table 70-4 VLL redundancy configuration options

Option	Configuration	Description
1	SAP SDP binding	You can create an endpoint without any SAP or SDP.
2	SAP SAP	You can create an endpoint without any SAP or SDP.
3	SDP binding SDP binding	You can configure this option for switching sites only.
4	SAP Endpoint with SDP bindings (maximum of 4 spokes and 1 ICB)	Figure 70-2 shows the configuration of this option on the PE nodes.
5	Endpoint with SAP/ICB SDP binding	Figure 70-3 shows the configuration of this option on Node B.
6	Endpoint with SAP/ICB endpoint with SAP/ICB	Figure 70-4 shows the configuration of this option.
7	Endpoint with SAP/ICB Endpoint with up to 4 SDP bindings	Figure 70-5 shows the configuration of this option.

Figure 70-2 VLL redundancy configuration - option 4

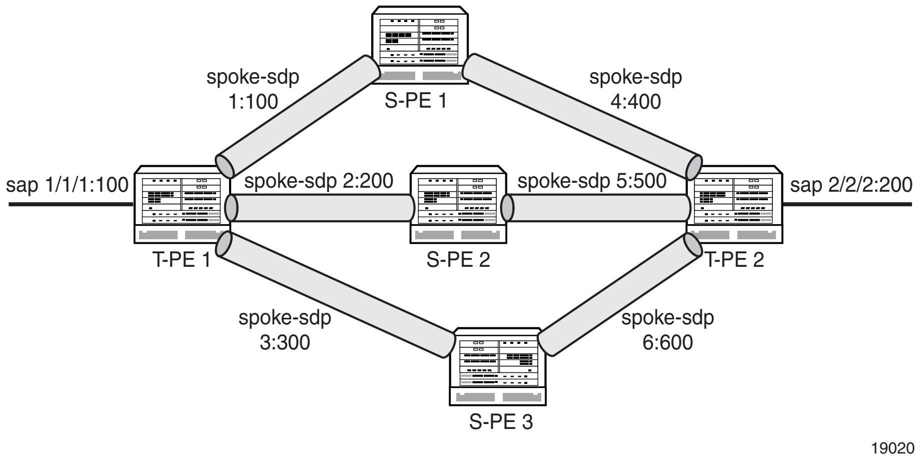


Figure 70-3 VLL redundancy configuration - option 5

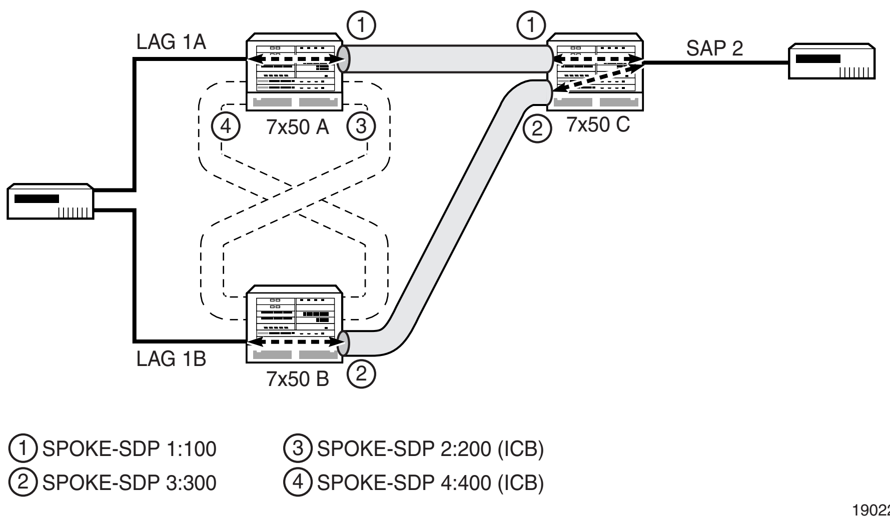


Figure 70-4 VLL redundancy configuration - option 6

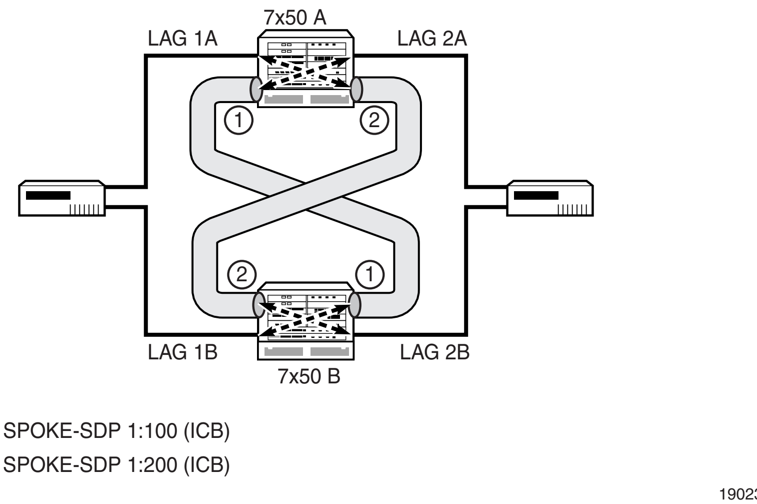
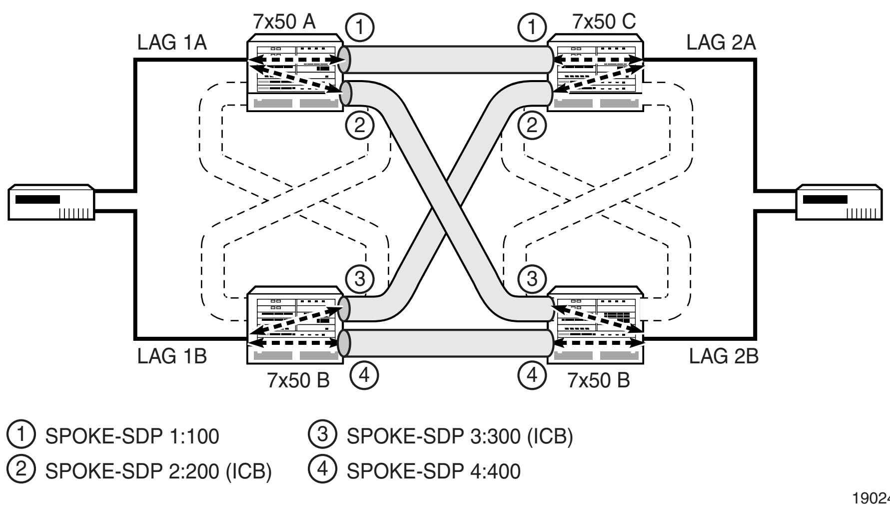


Figure 70-5 VLL redundancy configuration - option 7



Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching and redundancy:

- A VLL service can have one or more VLL instances. An instance can reside on a 7210 SAS-M, 7705 SAR, 7750 SR, 7450 ESS, or 7710 SR.
- Local endpoint rules:
  - A VLL instance has a maximum of two endpoints. A terminating VLL instance has at least one access endpoint and a switching VLL instance has two network endpoints.
  - A network endpoint has a maximum of four spoke-bindings, which can include any combination of the following: a single primary spoke, one or more secondary spokes with precedence, and one ICB spoke.
  - A SAP or a binding has a maximum of one endpoint association.
  - An endpoint has a maximum of one SAP.
  - A SAP or a binding with association to an endpoint can be moved to another endpoint or removed from that endpoint.
- SAP rules:
  - A MC-LAG SAP or MC-APS SAP cannot be deleted when there is an ICB on the same endpoint.
  - SAPs cannot exist on switching sites.
  - A maximum of two SAPs can exist for each site.
  - A SAP with a non-ICB spoke cannot exist on the same endpoint.
  - Apipe and Epipe services support MC-APS.
- Spoke binding rules:
  - The SDP types (GRE, MPLS) used by the redundant spoke bindings do not have to be the same when you manually create the spoke bindings.
  - Redundant configurations are not supported for S-PE because there are a maximum of two spoke bindings for a switching VLL instance.
  - An ICB SDP binding should not be created on an endpoint without a MC-LAG SAP or MC-APS SAP.
  - Only one ICB can exist for each endpoint.
  - ICB SDP binding can only have a precedence of 4, the lowest priority.
  - Only one primary spoke can exist for each endpoint.
  - Spoke SDP binding cannot associate with an endpoint on a switching site.
- HSDPA offload fallback rules:
  - Apipe and Epipe services support HSDPA offload fallback on ATM interfaces.
  - The spoke SDP must be configured with primary precedence.
  - The SAP must be configured with MC-APS or ATM channel.
  - When the SAP is configured with MC-APS, the spoke SDP can be configured with ICB.

HSDPA Offload Resiliency

Mobile service providers deliver both voice and data services to their customers using mobile handsets. The data services provided require significantly more bandwidth than voice services. In order to minimize the operational costs (specifically, bandwidth), service providers typically separate the voice and data traffic at the mobile base station. The voice traffic may be backhauled over an ATM infrastructure, while a Metro Ethernet infrastructure (their own or third-party) is used to backhaul the data traffic. The separation of data traffic onto a separate network for backhaul is referred to as High Speed Data-Link Packet Access offload.

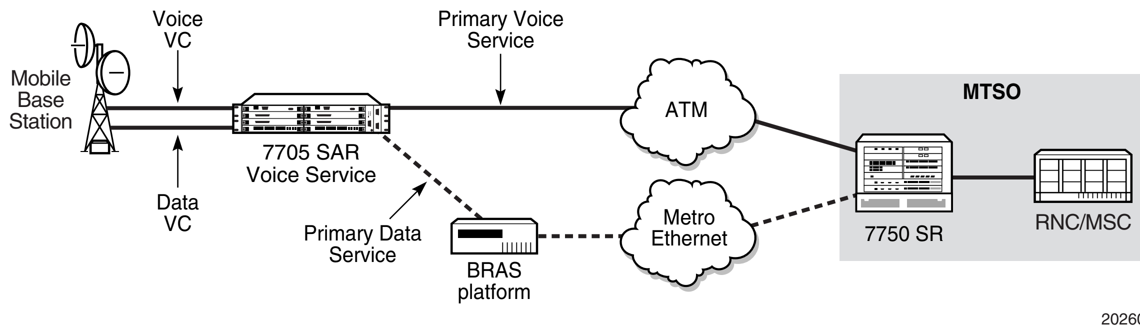
The HSDPA Apipe services traverse a path over the Metro Ethernet network which contains single potential points of failure that are unprotected. The ATM network can be used to provide a transient path for the data service in the event of a failure in the Metro Ethernet infrastructure, as long as the voice traffic is not impacted (data traffic is given lower QoS priority by the 7705 SAR and 7750 SR NEs). Clearly there is potential for the data service to suffer degradation (depending on the bandwidth required), until the fault in the Metro Ethernet network is resolved. However the SLA requirements for the data service are typically best effort.

The ability to switch to this alternate transient pathway for the data service is referred to as HSPDA resiliency.

HSPDA resiliency is implemented through the use of VLL Apipes on the 7705 SAR, Release 1.1 or later. The network architecture used in the ATM backhaul scenario is shown in Figure 70-6.

Note — For HSPDA offload resiliency, the primary and secondary services must be on the same NE.

Figure 70-6 ATM-based HSDPA offload architecture - nominal operation



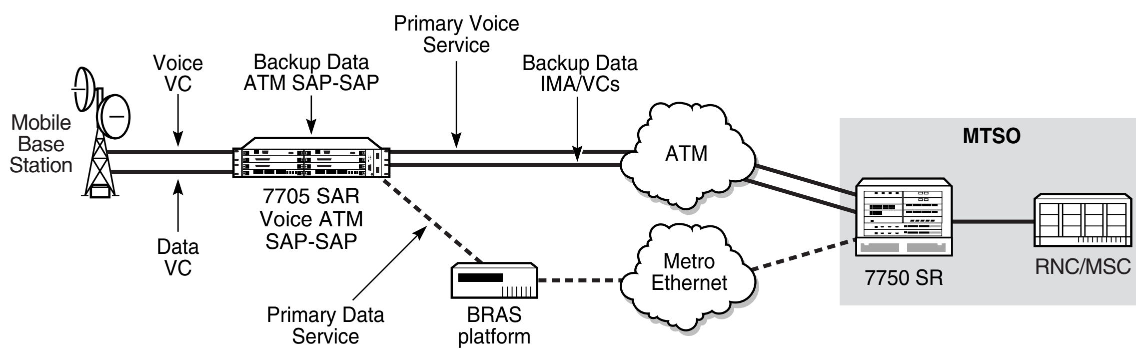
The mobile base station node separates the voice and data traffic and delivers the two different traffic types to the 7705 SAR on different VCs. Both the voice and data services use Apipe pseudo-wires to carry the traffic over the backhaul network to the 7705 SAR. The HSDPA Apipe service is paired with an OAM service (not shown in Figure 70-6) which is used by the wireless infrastructure to monitor the end-to-end path between the wireless endpoints.

For the ATM voice traffic, an internal Apipe is used on the 7705 SAR to switch ATM cells between the access VC/IMA group and the network side VC/IMA group. The service does not span the radio access network between the 7705 SAR and the 7750 SR located at the Mobile Telephone Switching Office (MTSO).

Data Apipe services (HSDPA/OAM) use service tunnels based on either MPLS or GRE. GRE is generally used in the context of a third-party Metro Ethernet network, since there is a Broadband Remote Access Server (BRAS) in the path between the DSLAM and the 7750 SR located at the MTSO (BRAS platforms do not support MPLS). MPLS is typically used when the mobile provider owns the Metro Ethernet network.

When the resiliency solution described below detects a failure in the Metro Ethernet network, its protection mechanism switches the traffic associated with the data service from the path over the Metro Ethernet network to a path which traverses the ATM (shown in Figure 70-7). The detection, switchover, and switchback mechanisms are implemented by the 5620 SAM.

Figure 70-7 HSDPA Offload Protection - ATM data backhaul



A backup (secondary) data service for an active (primary) data service is pre-configured on the 7705 SAR. For a typical 7705 SAR deployment at a cell site, two backup services are required, one for the HSDPA service and one for the OAM service. These backup services are created by the operator during the deployment of the 7705 SAR. A peer resiliency relationship between the active and backup services must also be configured.

The backup services used are internal Apipes. The switchover from primary to secondary is triggered by an event from the 7705 SAR sent to 5620 SAM, which indicates that the service tunnel (SDP) has failed. When the failure event is processed by 5620 SAM, the SAPs on the active data services are moved (along with the associated VCs) from the active service to its peer backup service and are enabled. After the re-configuration of the SAPs on the backup services completes, the traffic is moved to the backup services, which then carry the traffic over the ATM portion of the network. When the switchover is complete, an alarm is raised against the primary service indicating that it has been switched to the secondary service.

Other considerations include the following:

- If a service configured as primary is deleted from 5620 SAM or the CLI, then the corresponding resiliency is also deleted.
- If a service configured as secondary is deleted from 5620 SAM, this is blocked and a pop-up message indicates that the corresponding resiliency must first be deleted.
- If a service configured as secondary is deleted from the CLI, an alarm is raised indicating that the resiliency is misconfigured. If a secondary service is then subsequently added to the resiliency, this alarm is cleared.
- If the SAP initially configured on the primary service is deleted, the 5620 SAM raises an alarm. If the SAP is restored in the same service, the alarm clears.
- When the 5620 SAM detects that a failed SDP is up, which indicates that the primary service has recovered, the resiliency is set to the Secondary (Debounced) state and a damping timer is started. If the SDP goes down while the resiliency is in the Secondary (Debounced) state, the resiliency changes to the Secondary state and the damping timer stops. If the SDP changes state during the damping time, the value of the damping timer doubles until it rises to the maximum damping time. This prevents the service from flapping between primary and secondary. If the SDP does not change operational state during the damping time, the resiliency is set to Primary, the SAP is moved from the secondary to the primary service, and the alarm related to the service switch clears.
- After the primary service is restored, the damping timer value is set back to its initial value. The damping timer value is not displayed. The initial damping time is 30 000 ms; the time doubles, if required, to a maximum of 480 000 ms.
- The availability of this HSDPA resiliency feature is controlled by the 5620 SAM license key. If this feature is enabled using the 5620 SAM license key, then the Manage→Redundancy→HSDPA Resiliency feature is available on the main 5620 SAM menu, otherwise it does not appear. This feature also requires the SAM(P) module. A new package is added to the 5620 SAM License form called the Mobile Services Package. The HSDPA Resiliency feature is available when this package is enabled.

SDP bindings bandwidth allocation

You can administratively account for the bandwidth used by VLL services inside an RSVP SDP that consists of RSVP LSPs. The SR service manager keeps track of the available bandwidth for each SDP.

When you create a service tunnel, you configure an SDP Bandwidth Booking Factor percentage, which is applied to the SDP available bandwidth. You then assign an SDP Admin Bandwidth value (in kbps) to the spoke SDP. When you bind a VLL service to this SDP, this amount of bandwidth is subtracted from the adjusted available SDP bandwidth. If you subsequently delete the VLL service binding from this SDP, this bandwidth amount is added back into the adjusted SDP available bandwidth. If you overbook the total adjusted SDP available bandwidth when adding a VLL service, a warning is issued and the binding is rejected.

This feature does not guarantee bandwidth to a VLL service, as there is no change to the data path to enforce the bandwidth of an SDP by means such as shaping or policing of the constituent RSVP LSPs. Also, this feature does not provide a CAC capability for a local VLL service which consists of a cross-connect between two SAPs.

In addition, if multipoint services such as VPLS and VPRN are using the same SDP for forwarding packets, the amount of bandwidth consumed by these services is also not accounted for. Therefore, it is advisable to dedicate an SDP for VLL services for which bandwidth reservation is required. Furthermore, VPLS and VPRN services which use separate SDPs but which forward packets over the same network port as the VLL SDP also do not have their bandwidth accounted for. This may impact the bandwidth available to the VLL services.

Auto SDP binding (for all spoke bindings or just the return binding) cannot be used when there is a bandwidth request for the binding. The converse also applies. An error message appears when saving the configuration if this conflict occurs. 5620 SAM checking is done for OSSI.

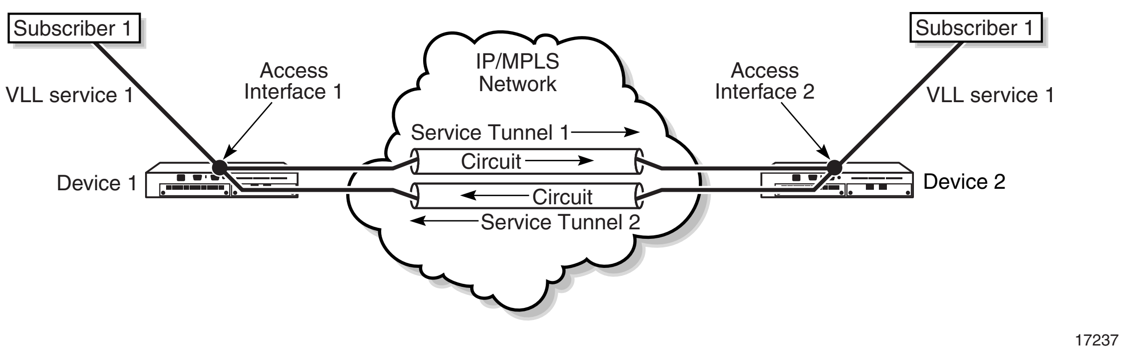
Copying and moving SAPs between ports

You can copy and move SAPs between ports. See section “Moving and copying SAPs between ports” in chapter 20 for more information.

70.2 Sample VLL service

Figure 70-8 shows a sample VLL service.

Figure 70-8 Sample VLL service



Assuming the core IP/MPLS network and service tunnels have already been configured, Table 70-5 shows the high-level tasks required to configure this sample VLL service.

Table 70-5 Sample VLL service configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies is defined when you configure or modify resources such as access interfaces during VLL service creation or modification. The following key policies can be applied to resources that are part of a VLL service. • Access ingress and egress interface policies, or ATM policies. Choose Policies→QoS→SROS QoS→Access Ingress, Access Egress, or ATM QoS to open these forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL IP and ACL MAC filter policies. Choose Policies→Filter→ACL IP Filter or ACL MAC Filter to open the filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
2. Configure ports as access ports for use in the service	If applicable, choose a port from the navigation tree, right-click on the port, and choose Properties from the contextual menu. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Service tunnels are automatically created if there are no tunnels between the source and destination devices. You must choose GRE as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Unidirectional service tunnels carry service traffic between edge managed devices using aggregated SDP bindings. SDP bindings can be associated with service tunnels during service configuration. During service creation, you can also configure the 5620 SAM to automatically create and associate service tunnels with SDP bindings. In this case, you do not have to create service tunnels before you create the service. After you have created a VLL, status indicators display selected operational failures on the service tunnel and peer SAP.
4. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

5. Create and configure Service 1	Choose Create→Service→VLL→*Type of VLL service*. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Associate Subscriber 1 with the service.
	• Specify Device 1 and Device 2 as the sites for the VLL service.
	• Configure and specify Access Interface 1 and Access Interface 2 as the access interfaces for the VLL service. You do the following when you configure access interfaces.
	  • Specify the ports for the access interfaces. Ethernet ports must be configured as access ports.
	  • Specify participation of the access interfaces in access ingress, access egress, and ATM QoS policies as required.
	  • Specify participation of the access interfaces in aggregation rate limiting across a card or port. If aggregation is not required, specify participation of the access interfaces in ingress and egress scheduler policies. If aggregation is required, specify participation of the access interfaces in an aggregation scheduler policy.
	  • Specify participation of the access interfaces in scheduler policies as required.
	  • Set the ATM OAM Terminate parameter to Up when the VLL L2 access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU.
	Create and configure circuits in both directions. Associate the circuit from Device 1 to Device 2 with Service Tunnel 1. Associate the circuit from Device 2 to Device 1 with Service Tunnel 2. You can also configure the 5620 SAM to automatically create and associate service tunnels with circuits.

70.3 Workflow to create a VLL service

The following workflow lists the high-level steps required to create a VLL service. As a prerequisite for creating a VLL service, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1.
- the access ports for the service are created; see chapter 20 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.

1 Create and configure the VLL service:

i Define the VLL service type as Epipe, Apipe, Fpipe, Hpipe, Ipipe, or Cpipe.

- For VLL Epipe services:
  - For all devices that support the creation of a VLL service except for 7210 SAS or 9500 MPR devices, see Procedure 70-1.
  - For 7210 SAS devices, see Procedure 70-2.
  - For 9500 MPR (ANSI only) devices, see Procedure 70-3.
- For VLL Apipe services:
  - For all devices that support the creation of a VLL service except for 9500 MPR devices, see Procedure 70-4.
  - For 9500 MPR (ETSI only) devices, see Procedure 70-5.
- For VLL Fpipe services, see Procedure 70-6.
- For VLL Hpipe services, see Procedure 70-7.
- For VLL Ipipe services, see Procedure 70-8.
- For VLL Cpipe services:
  - For all devices that support the creation of a VLL service except for 9500 MPR devices, see Procedure 70-9.
  - For 9500 MPR (ETSI and ANSI) devices, see Procedure 70-10.

ii Specify the devices (sites) used in the service based on the following topologies:

- Traditional VLL: terminating site only
- Switching VLL: switching site with two or more terminating sites
- Redundant VLL: ICB spoke to MC-LAG (Epipe) or MC-APS (for Apipe and Epipe)

iii Specify the following information for redundant VLL services:

- endpoints
- access interfaces for VLL terminating sites

iv Specify the following information to create a VLL Apipe or Epipe HSDPA offload fallback solution:

- endpoints
- SAP on endpoint one with MC-APS or ATM channel
- spoke SDP with ICB on endpoint one
- spoke SDP with primary precedence on endpoint two
- SAP on endpoint two with MC-APS
- spoke SDP with ICB on endpoint two

v Specify aggregation on a service basis, or across a card or port.

vi Specify QoS, scheduling, accounting, ANCP, MEP association and filter policies.

vii Specify the time of day suite.

2 For VLL services created on a 9500 MPR or OmniSwitch, if required:

a Create VLAN groups and add members to each group as required. See Procedure 69-10.

b Delete a VLAN group or group member. See Procedure 69-11.

3 For VLL services created on a 9500 MPR, if required:

a Create the VLAN paths that are required between the 9500 MPR group members. The VLAN path can be hop based or ring based. See Procedure 69-12.

b Delete a 9500 MPR VLAN path. See Procedure 69-13.

c Fix a failed cross-connection in a 9500 MPR Cpipe. See Procedure 70-11.

4 Turn up the service.

5 Perform one or more of the following as required.

a Configure a GNE site on a VLL service. See Procedure 70-12.

b Create a VLL L2 access interface on a terminating site. See Procedure 70-13.

c Create a SAP aggregation group for a 7705 SAR Apipe. See Procedure 70-14.

d Create an HSDPA resiliency configuration. See Procedure 70-15.

e Activate and manually operate an HSDPA resiliency configuration. See Procedure 70-16.

f Run an OAM validation test for a VLL service. See Procedure 70-17.

6 As required, view VLL information:

  a View the service topology map associated with a VLL service. See Procedure 70-18.

  b View the VLL service operational status. See Procedure 70-19.

  c View the peer status information associated with the VLL service. See Procedure 70-20.

7 As required, modify a VLL service:

  a Using the Manage Services form. See Procedure 70-21.

  b Using the topology view. See Procedure 70-22.

8 As required, delete a VLL service. See Procedure 70-23.

70.4 VLL service management procedures

Use the following procedures to perform VLL service creation and management task

Procedure 70-1 To create a VLL Epipe service

1 Choose Create→Service→VLL→Epipe (Ethernet to Ethernet/ATM/FR/CEM) from the 5620 SAM main menu. The Epipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL Epipe service. The Select Customer - Epipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Epipe Service form closes and the Epipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.
  The CAC Status, CAC Probable Cause, and Last CAC Time fields are visible if service CAC has been configured. See step 48 for more information. The Last CAC Time field displays the last time that a CAC verify or CAC audit was run.

5 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

6 Perform one of the following:

a Choose a site for the VLL service. Go to step 7.

b Complete the VLL service creation if the sites and interfaces are to be created later. Go to step 52.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

7 On the navigation tree, right-click on VLL Epipe and choose Create Epipe Site. The Select Network Elements - VLL Epipe form opens with a list of available sites.

8 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- MTU Check
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled
- VLL Site Type
- Tunnel Fault Notification

The VLL Site Type parameter is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the facility tunnel MEP.

10 Click on the Apply button.

11 Perform one of the following:

a Link the site to a Backbone VPLS. Go to step 12.

b Create endpoints for a redundant VLL. Go to step 14.

Note — Redundant VLL Epipe services are configurable on the 7705 SAR, 7450 ESS, 7750 SR, and 7710 SR.

c Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.

d Create a spoke SDP binding for the site. Go to step 20.

e Create a spoke SDP FEC for the site. Go to step 41.

f Complete site creation. Go to step 49.

12 Choose the Backbone VPLS site to link the Epipe service to. For additional information on Provider Backbone Bridging, see chapter 71.

i Click on the Backbone tab button.

ii Click on the Select button. The Select Backbone VPLS Site - Site form is displayed.

iii Click the Search button. A list of all the B-Sites that can be used by the Epipe is displayed. You can narrow the search by using the using the filtered properties shown in the form.

Note — The B-Sites listed are only those that are on the same node as the Epipe site.

iv Choose a B-VPLS and click on OK. The Select Backbone VPLS Site - Site form closes and the Service ID of the chosen B-VPLS appears on the Site (Create) form.

Note — The selection of a B-Site in this step must be repeated for both Epipe sites you create. You must select a B-Site that is on the same node as the Epipe site you are creating.

v In the PBB block, configure the following parameters:

- ISID
- Destination MAC Address or MAC Name

Note 1 — The ISID parameter should be set to the same value for both Epipe sites you create for this service.

Note 2 — To select a previously created Mac Name, click on the Select button and select a MAC Name from the list in the Select MAC Destination MAC Address Alias window. See Procedure 17-10 for more information on how to create a MAC Name.

Note 3 — The Destination MAC Address or MAC Name parameter you set for this Epipe site should be the same as the Source MAC Address of the B-Site on the other node of the Epipe service you are creating.

vi Configure the Force Q Tag Forwarding parameter.

vii Click on Apply. The Operational Destination MAC Address is updated with the configured Destination MAC Address or MAC Address associated with the selected MAC Name.

13 If you are creating an Epipe service linked to a Backbone VPLS go to step 18.

14 On the navigation tree, right-click on Endpoints and choose Create Endpoints. The Endpoint (Create) form opens.

15 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)
- Enable PW Standby Signaling Master
- Enable PW Standby Signaling Slave

16 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 14 through 16 for each endpoint in the VLL service.

17 Click on the Apply button.

18 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 70-13.

Note 1 — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces can be on LAGs that participate in the MC LAG, or they can be just regular or Ethernet tunnel access interfaces.

Note 2 — If the Use SAP Backbone MAC Address parameter is enabled on both B-Sites then:

- MC-LAG access interfaces for the PBB Epipe local switching must be on IOM3 MDAs for the feature to work properly. There is no 5620 SAM or CLI validation.
- Other access interfaces may be on IOM1 or IOM2 MDAs.

b Create a spoke SDP binding for the site. Go to step 20.

c Complete site creation. Go to step 49.

19 If you are creating an Epipe service linked to a Backbone VPLS go to step 49.

20 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

21 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

22 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

23 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

24 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

25 When you set the Precedence parameter to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.

26 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- Enable PW Status Signaling
- Enable PW Standby Signaling Slave
- Force VLAN VC Forwarding
- SDP Admin Bandwidth

27 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 26.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

28 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

29 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VLL service form displays only local profiles on the NE.

30 Associate an AA transit prefix policy with the service object, if required.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

31 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

32 Click on the States tab button.

33 Configure the Administrative State parameter.

34 Click on the Pseudowire OAM tab button.

35 Configure the Control Word parameter.

36 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

37 Assign an accounting policy to the SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Choose an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the accounting policy information displayed.

38 Associate a MEP to the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- CCM Messages Enabled
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The MEP (Create) form closes.

39 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

40 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

A VLL with spoke switching requires that there is a switching site and two or more terminating sites. Repeat steps 20 through 40 to define the sites required for your VLL configuration.

41 On the navigation tree, right-click on Spoke SDP FECs and choose Create Spoke SDP FEC. The Spoke SDP FEC (Create) form opens. Complete steps 42 through 47 to configure a spoke SDP FEC.

42 Configure the PW ID parameter or enable the Auto-Assign ID parameter.

43 On the Source panel, do the following:

i Click on the Select button next to the SAII Address field and select an SAII address.

ii Configure the SAII AC ID parameter.

44 On the Target panel, do one of the following:

a Configure the Auto Config parameter.

b Do the following:

i Click on the Select button next to the TAII Address field and select a TAII address.

ii Configure the TAII AC ID parameter.

45 On the General Parameters panel, do the following:

i Configure the parameters.

- Administrative State
- Signalling Type
- Retry Timer
- Retry Counter

ii Click on the Select button next to the Path field and select a path.

iii Click on the Select button next to the PW Template field and select a PW template.

46 On the Redundancy panel, do the following:

i Click on the Select button next to the Endpoint field and select an endpoint.

ii Configure the parameters.

- Inter-Chassis Backup
- Precedence
- Active State

47 On the Pseudowire Signalling panel, configure the Enable PW Standby Signaling Slave parameter.

48 To configure bandwidth for the service if required, click on the Bandwidth tab and proceed as follows:

Note — The Bandwidth tab is only available if service CAC is configured; see chapter 6 for information about enabling and disabling service CAC.

i For each CoS, enter the value for the Reserved Bandwidth, as required.

ii Click on the General tab to determine the CAC status.

If the Verify CAC button is enabled, the CAC has not been verified. The Probable Cause and CAC Status fields provide details.

The CAC Status field describes the current CAC status of the service. CAC statuses are as follows.

- CAC Verified indicates that all tunnels have sufficient bandwidth to admit service and that requested bandwidth for the service is booked on the appropriate physical links.
- CAC Failed indicates that the attempt made to admit service into the network was unsuccessful. The most likely cause for this is insufficient bandwidth. See the Probable Cause field for more specific information.
- BW Defined, No CAC Request indicates that the required bandwidth is defined on the service; however, a CAC request has not occurred.
- CAC To be Verified indicates that a tunnel has been configured on the service either manually or through the CLI; however, the required bandwidth has not been verified in the network.

The Probable Cause field describes possible reasons for the current CAC state. Probable causes are as follows.

- No Candidate Tunnels Found indicates that the autobind tunnel function was found, but no suitable tunnels were found.
- Different PBB Tunnels Applied to Service indicates that two or more different PBB tunnels are configured on this service.
- Not Enough Bandwidth on any Candidate Tunnels indicates that one or more candidate tunnels were found, but the available bandwidth was insufficient to admit the service.
- Automatic PBB Tunnel Selection Failed indicates that a suitable PBB tunnel was found, but there were errors when attempting to assign the tunnel to the service. A dialog box will provide more details.
- Site Missing Tunnel indicates that at least one selected site is not configured with a PBB tunnel.
- All PBB Tunnels have not been Verified indicates that all sites within the service have a tunnel configured, but the available bandwidth has not been booked or verified in the network.

iii To manually verify the CAC, click on the Verify CAC button if it is enabled. The 5620 SAM will attempt to find the most appropriate PBB tunnel for the service-based on available bandwidth, and to automatically bind the tunnel to the service if one has not already been assigned.

49 Click on the OK button. The Site (Create) form closes and a dialog box appears.

50 Click on the OK button. The VLL Epipe (Create) form reappears with the new information displayed in the service navigation tree.

51 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 7 to 50.

b Complete service creation. Go to step 52.

52 Click on the OK button. The VLL Epipe (Create) form closes.

You can use the topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-2 To create a VLL Epipe service on a 7210 SAS device

1 Choose Create→Service→VLL→Epipe (Ethernet to Ethernet/ATM/FR/CEM) from the 5620 SAM main menu. The Epipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Epipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Epipe Service form closes and the Epipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

6 On the navigation tree, right-click on VLL Epipe and choose Create Site. The Select Network Elements - VLL Epipe form opens with a list of available sites.

7 Perform one of the following:

a Choose a 7210 SAS and click on the OK button. The Site (Create) form opens with the General tab displayed. Continue to step 8.

b Choose a non-7210 SAS terminating site that is physically connected to the 7210 SAS by a port or a LAG and click on the OK button. The Site (Create) form opens with the General tab displayed. Go to step 13.

Note — The non-7210 SAS terminating sites typically are a 7450 ESS, 7750 SR, or 7710 SR.

8 Configure the parameters:

- Name
- Description
- MTU
- MTU Check
- Administrative State
- SAP Type
- Monitor Access Interface Operational State
- PBB Epipe

The PBB Epipe parameter is only configurable on the 7210 SAS-M and 7210 SAS-X.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button.

11 If you enabled the PBB Epipe parameter in step 8, choose the Backbone VPLS site to link the Epipe service to. For additional information on Provider Backbone Bridging, see chapter 71.

i Click on the Backbone tab button.

ii Click on the Select button. The Select Backbone VPLS Site - Site form is displayed.

iii Click the Search button. A list of all the B-Sites that can be used by the Epipe is displayed. You can narrow the search by using the using the filtered properties shown in the form.

Note — The B-Sites listed are only those that are on the same node as the Epipe site.

iv Choose a B-VPLS and click on OK. The Select Backbone VPLS Site - Site form closes and the Service ID of the chosen B-VPLS appears on the Site (Create) form.

Note — The selection of a B-Site in this step must be repeated for both Epipe sites you create. You must select a B-Site that is on the same node as the Epipe site you are creating.

v In the PBB block, configure the following parameters:

- ISID
- Destination MAC Address or MAC Name

Note 1 — The ISID parameter should be set to the same value for both Epipe sites you create for this service.

Note 2 — To select a previously created Mac Name, click on the Select button and select a MAC Name from the list in the Select MAC Destination MAC Address Alias window. See Procedure 17-10 for more information on how to create a MAC Name.

Note 3 — The Destination MAC Address or MAC Name parameter you set for this Epipe site should be the same as the Source MAC Address of the B-Site on the other node of the Epipe service you are creating.

vi Click on Apply. The Operational Destination MAC Address is updated with the configured Destination MAC Address or MAC Address associated with the selected MAC Name.

12 Go to step 14.

13 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

You can only configure the VLL Site Type parameter when the terminating site is a 7450 ESS, 7710 SR, or 7750 SR.

Note — The site must be exclusively terminating, when physically connected to the 7210 SAS.

14 On the navigation tree, right-click on Access Interfaces below the site and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

Note — If 7210 SAS-D 6F 4T ETR or 7210 SAS-E sites are connected in a ring network, you must configure an Uplink SAP between the sites.

15 Configure the parameters:

- Description
- Administrative State

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

19 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Transit SAP

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button.

22 The L2 Access Interface (Create) form closes.

23 Close the Epipe Service (Create) form.

Procedure 70-3 To create a VLL Epipe service on the 9500 MPR (ANSI only)

1 Choose Create→Service→9500 VLL→Epipe (ETH to Eth) from the 5620 SAM main menu. The Epipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Epipe service. The Select Customer - Epipe Service form opens.

3 Choose the Default Customer as the customer for the Epipe service and click on the OK button. The Select Customer - Epipe Service form closes and the Epipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Specify VLAN Path
- OLC State
  This parameter is configurable when you click on the Apply button.

5 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

6 Click on the main General tab button.

7 Click on the Select button to choose a VLAN path to associate with the Epipe service. The Select VLAN Path - Epipe Service form opens.

Note — If no VLAN path exists, see Procedure 69-12 for more information about how to create VLAN paths.

8 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Epipe Service form closes and the Epipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

9 Configure the parameters:

- Auto-Assign ID
- VLAN ID

The VLAN ID parameter is enabled when the Auto-Assign ID parameter is disabled.

Note — The CEM to Eth Service Class is set automatically and is read-only.

10 Configure the parameter:

- Clock Source

11 On the navigation tree, right-click on an Epipe Site and choose Create Epipe Site. The Epipe Site (Create) form opens with the General tab displayed.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

12 Configure the parameters:

- Name
- Description

13 On the navigation tree, right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Auto-Assign ID
- Mac Address
- Monitor Access Interface Operational State

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists Ethernet ports in access mode.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

18 Click on the OK button. A dialog box appears.

19 Click on the OK button. The L2 Access Interface (Create) form closes, and the Epipe Site (Create) form reappears with the new interface information displayed in the service navigation tree.

20 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 11 to 17.

b Complete service creation. Go to step 21.

Note 1 — The backhaul service is extended to include the far end points when the 9500 MPR is paired with the 7705 SAR or 7210 SAS nodes. These nodes are called Termination Points (TPs). The far end node could be any of the above nodes which are fully managed by the 5620 SAM. The TP is a permanent object of an 9500 MPR VLL; when the service is within the 9500 MPR network, the TP would point to SAPs on the 9500 MPR, when the services are extended or terminated on other nodes then it points to the far end points of the 7705 SAR or 7210 SAS devices. The TPs improve alarm aggregation or correlation and they would be displayed in the service topology.

Note 2 — Whenever a non-MPR node is connected to the 9500 MPR through a physical link, you can change the mode of the 9500 MPR Ethernet port from Access to Network. However, if the 9500 MPR port is part of the L2 Access interface, then the mode cannot be changed from Access to Network.

21 Click on the OK button. The VLL Epipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-4 To create a VLL Apipe service

VLL Apipe services are configurable only on the 7450 ESS in mixed mode, 7750 SR, 7710 SR, and 7705 SAR.

1 Choose Create→Service→VLL→Apipe (ATM to ATM/FR) from the 5620 SAM main menu. The Apipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Apipe Services form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Apipe Service form closes and the Apipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- SVC Mgr Service ID
- Default VC ID
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type
- OLC State

The Service ID and SVC Mgr Service ID parameters are configurable when the Auto-Assign ID parameter is disabled. The Default VC ID parameter is configurable when the Inherit Service ID Value parameter is disabled. The Profile Name parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank. The OLC State parameter is configurable when you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 32.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

6 On the navigation tree, right-click on VLL Apipe and choose Create Apipe Site. The Select Network Elements - VLL Apipe form opens with a list of available sites.

7 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type
- Interworking Type
- Signalling VC Type Override

The VLL Site Type parameter is configurable only on the 7450 ESS and 7750 SR.

9 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 10.

Note — Redundant VLL Apipe services are configurable on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.

c Create a spoke SDP binding for the site. Go to step 15.

d Complete site creation. Go to step 33.

10 On the navigation tree, right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

11 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

12 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 10 through 12 for each endpoint in the VLL service.

13 Click on the Apply button.

14 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 70-13.

b Create a SAP aggregation group with L2 access interfaces for the VLL terminating sites. Perform Procedure 70-14.

c Create a spoke SDP binding for the site. Go to step 15.

d Complete site creation. Go to step 33.

15 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

16 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

17 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth

18 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM blocks the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

19 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

20 When you set the Precedence parameter to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.

21 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 17.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

22 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

23 Click on the States tab button.

24 Configure the Administrative State parameter.

25 Click on the Pseudowire OAM tab button.

26 Configure the Control Word parameter.

If you set the VC Type parameter to ATM-SDU in step 4, you must set the Control Word parameter to Preferred.

27 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

28 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

29 Click on the OK button. The Site (Create) form closes and a dialog box appears.

30 Click on the OK button. The VLL Apipe (Create) form reappears with the new information displayed in the service navigation tree.

31 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 30.

b Complete service creation. Go to step 32.

32 Click on the OK button. The VLL Apipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

33 If required, modify the SDP binding parameters for ATM cell concatenation.

i Open and modify the Apipe configuration form, as described in Procedure 70-21.

ii Click on the Spoke SDP Binding tab.

iii Choose a SDP binding from the list and click on the Properties button.

iv Click on the ATM tab.

v Configure the parameters:

- AAL5 Frame Aware
- Admin Concat Limit
- Max Concat Delay
- CLP Change

vi Save the changes and close the Apipe configuration form.

Procedure 70-5 To create a 9500 MPR Apipe service (ETSI only)

1 Choose Create→Service→9500 VLL→Apipe (ATM to ATM/Eth) from the 5620 SAM main menu. The Apipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Apipe service. The Select Customer - Apipe Service form opens.

3 Choose the Default Customer as the customer for the Apipe service and click on the OK button. The Select Customer - Apipe Service form closes and the Apipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Specify VLAN Path
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Click on the Select button to choose a VLAN path to associate with the Apipe service. The Select VLAN Path - Apipe Service form opens.

6 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Apipe Service form closes and the Apipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

Note — If no VLAN path exists, see Procedure 69-12 for more information about how to create VLAN paths.

7 Configure the parameters:

- VLAN ID
- Auto-Assign ID
- Service Class
- PW Label
- Auto-Assign ID
- VC Type

The VLAN ID and PW Label parameters are enabled when the Auto-Assign ID parameters are disabled.

8 If you specified the ATM to Eth option in step 7, configure the MAC Address parameter.

9 On the navigation tree, right-click on an Apipe Site. The Apipe Site (Create) form opens with the General tab displayed.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

10 Configure the parameters:

- Name
- Description

11 On the navigation tree, right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

12 Configure the parameters:

- Name
- Description

13 Click on the Port tab button.

14 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

15 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

Note 1 — If ports on a card slot of the 2+2 x Ethernet (EAS) card are used to create the Apipe service, first configure the Profile Name parameter on the card slot. See Procedure 20-29 for more information on configuring this parameter.

Note 2 — If MPT-MC or MPT-HC ports are being used as network ports on the 2+2 x Ethernet (EAS) card, then the peer MAC Address must be specified for the L2 Access Interface.

16 Do one of the following.

a If you selected a value of VCC for the VC Type parameter, go to step 17.

b If you selected a value of VPC for the VC Type parameter, go to step. 19.

17 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value (VCI)
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

18 Go to step 20.

19 Configure the parameters:

- Outer Encapsulation Value
- Outer Encapsulation Value (VPI)

20 Click on the ATM tab button.

21 Click on the Select button to choose an Ingress ATM Policy. The Select Ingress ATM Policy - ATM Configuration form opens.

22 Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the L2 Access Interface (Create) form displays the policy information.

23 Click on the Select button to choose an Egress ATM Policy. The Select Egress ATM Policy - ATM Configuration form opens.

24 Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the L2 Access Interface (Create) form displays the policy information.

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The L2 Access Interface (Create) form closes, and the Apipe Site (Create) form reappears with the new interface information displayed in the service navigation tree.

27 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 11 to 20.

b Complete service creation. Go to step 28.

28 Click on the OK button. The VLL Apipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Note — In case of a service creation failure and/or generated NE inconsistencies, see Procedure 37-21.

Procedure 70-6 To create a VLL Fpipe service

1 Choose Create→Service→VLL→Fpipe (FR to FR) from the 5620 SAM main menu. The VLL Fpipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Fpipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Fpipe form closes and the VLL Fpipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 31.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

6 On the navigation tree, right-click on VLL Fpipe and choose Create Fpipe Site. The Select Network Elements - VLL Fpipe form opens with a list of available sites.

7 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

The VLL Site Type parameter is configurable only on the 7450 ESS, 7750 SR, and 7705 SAR.

9 Perform one of the following:

- **a** Create endpoints for a redundant VLL. Go to step 10.
- **b** Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.
- **c** Create a spoke SDP binding for the site. Go to step 15.
- **d** Complete site creation. Go to step 33.

10 On the navigation tree, right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

11 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

12 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 10 through 12 for each endpoint in the VLL service.

13 Click on the Apply button.

14 Perform one of the following:

- **a** Create an L2 access interface for the VLL terminating sites. Perform Procedure 70-13.
- **b** Create a spoke SDP binding for the site. Go to step 15.
- **c** Complete site creation. Go to step 33.

15 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

16 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

17 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label

18 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

19 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

20 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- SDP Admin Bandwidth

21 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 20.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

22 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

23 Click on the States tab button.

24 Configure the Administrative State parameter.

25 Click on the Pseudowire OAM tab button.

26 Configure the Control Word parameter.

If you set the VC Type parameter to FR-DLCI in step 4, you must set the Control Word parameter to Preferred.

27 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.

28 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

29 Click on the OK button. The Site (Create) form reappears with the new information displayed in the service navigation tree.

30 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 29.

b Complete service creation. Go to step 31.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The VLL Fpipe (Create) form reappears.

33 Click on the OK button. The VLL Fpipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-7 To create a VLL Hpipe service

VLL Hpipe services are configurable only on the 7705 SAR and 7705 SAR-M (version 5.0 and later).

In order to configure a VLL Hpipe service on a supporting NE, the daughter card MDA Mode must be set to cem-fr-hdlc-ppp. For more information, see Procedure 19-24. Only ports that are configured with an Encap Type of HDLC can be mapped to an Hpipe SAP. For more information, see Procedure 20-1.

1 Choose Create→Service→VLL→Hpipe (HDLC to HDLC) from the 5620 SAM main menu. The Hpipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL Hpipe service. The Select Customer - Hpipe Service form opens.

3 Choose a customer for the VLL Hpipe service and click on the OK button. The Select Customer - Hpipe Service form closes and the Hpipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Perform one of the following:

a Create a site for the Hpipe. Go to step 6.

b Complete Hpipe creation if sites and interfaces are to be created later. Go to step 28.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

6 On the navigation tree, right-click on Hpipe Service and choose Create Hpipe Site. The Select Network Elements - Hpipe form opens with a list of available sites.

7 Choose a site and click on the OK button. The Hpipe Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- MTU Check
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

9 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 10.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.

c Create a spoke SDP binding for the site. Go to step 14.

d Complete site creation. Go to step 30.

10 Click on the Endpoints tab and then click on the Create button. The Endpoint (Create) form opens.

11 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Enable PW Standby Signaling Master
- Enable PW Standby Signaling Slave

12 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 10 through 12 for each endpoint in the VLL service.

13 Click on the Apply button.

14 Click on the Spoke SDP Bindings tab and then click on the Create button. The Spoke SDP Binding form opens with the General tab displayed.

15 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

16 Configure the parameters:

- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label

17 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

18 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Precedence
- Active State

19 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab button does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 20.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

20 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

21 Click on the States tab button.

22 Configure the Administrative State parameter.

23 Click on the Pseudowire OAM tab button.

24 Configure the Control Word parameter.

If you set the VC Type parameter to HDLC in step 4, you must set the Control Word parameter to Preferred.

25 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

26 Click on the OK button. The Hpipe Site (Create) form reappears with the new information displayed in the service navigation tree.

27 Perform one of the following:

- **a** Create an additional site for the VLL service, if required. Repeat steps 6 to 26.
- **b** Complete service creation. Go to step 28.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The VLL Hpipe (Create) form reappears.

30 Click on the OK button. The VLL Hpipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-8 To create a VLL Ipipe service

1 Choose Create→Service→VLL→Ipipe from the 5620 SAM main menu. The Ipipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Ipipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Ipipe Service form closes and the Ipipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- Use Bandwidth-Reserved Paths
- OLC State
  This parameter is configurable when you click on the Apply button.

5 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

6 Perform one of the following:

a Create a site for the VLL. Go to step 7.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 40.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

7 On the navigation tree, right-click on Ipipe Service and choose Create Ipipe Site. The Select Network Elements - Ipipe Service form opens with a list of available sites.

8 Choose a site and click on the OK button. The Ipipe Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type
- Enable CE IP Address Discovery
- Enable IPv6
- Stack Capability Signaling
- Tunnel Fault Notification

The VLL Site Type parameter is configurable only on the 7450 ESS, 7750 SR, and 7705 SAR.

The Enable CE IP Address Discovery parameter is configurable only for VLL terminating sites.

The Enable IPv6 parameter is configurable only when the Enable CE IP Address Discovery parameter is enabled.

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault notification from the facility tunnel MEP.

Note — The IPv6 capability is only supported on the 7450 ESS in mixed mode (chassis mode D and above), 7710 SR (chassis mode C and above), and 7750 SR (chassis mode C, and chassis modes A and B with mixed mode enabled).

The Stack Capability Signaling parameter is configurable only when the Enable IPv6 parameter and the Enable CE IP Address Discovery parameters are enabled.

10 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 11.

Note — Redundant VLL Ipipe services are configurable only on the 7705 SAR, 7450 ESS, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.

c Create a spoke SDP binding for the site. Go to step 17.

d Complete site creation. Go to step 36.

11 On the navigation tree, right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

12 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

13 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

14 Repeat steps 11 to 13 for each endpoint in the VLL service.

15 Click on the Apply button.

16 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 70-13.

b Create a spoke SDP binding for the site. Go to step 17.

c Complete site creation. Go to step 36.

17 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

18 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

19 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- VC Type
- Ingress Label
- Egress Label

20 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

21 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

22 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- SDP Admin Bandwidth

23 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required:

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameters.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 22.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

24 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

25 Choose an Application Profile for the spoke SDP binding.

- **i** Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.
- **ii** Configure the filter criteria. A list of Application Profiles appears.
- **iii** Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding service form displays only local profiles on the NE.

26 Associate an AA transit prefix policy with the service object, if required.

- **i** Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.
- **ii** Select a transit IP policy and click on the OK button.

27 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

- **i** Click on the 5670 RAM Parameters tab button.
- **ii** Click on the Reporting tab button.
- **iii** Click on the Create button. The AA Reporting (Create) form opens.
- **iv** Configure the parameters:
  - Customer Name
  - Subscriber Class
  - Total Bandwidth Upstream (Kbps)
  - Class of Service 1 Bandwidth Upstream (Kbps)
  - Class of Service 2 Bandwidth Upstream (Kbps)
  - Class of Service 3 Bandwidth Upstream (Kbps)
  - Class of Service 4 Bandwidth Upstream (Kbps)
  - Subscriber Name
  - Subscriber Type
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
- **v** Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.
- **vi** Click on the General tab button.

28 Click on the States tab button.

29 Configure the Administrative State parameter.

30 Click on the Pseudowire OAM tab button.

31 Configure the Control Word parameter.

32 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

- **i** Click on the ACL tab button.
- **ii** Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.
- **iii** Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.
- **iv** Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.
- **v** Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.
- **vi** Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.
- **vii** Choose an IPv6 ingress filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 ingress ACL filter information displayed.
- **viii** Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.
- **ix** Choose an IPv6 egress filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 egress ACL filter information displayed.

33 Click on the Ipipe tab button.

34 Configure the Peer CE IP Address parameter.

35 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

36 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

37 Click on the OK button. The Site (Create) form closes and a dialog box appears.

38 Click on the OK button. The VLL Ipipe (Create) form reappears with the new information displayed in the service navigation tree.

39 Perform one of the following:

- **a** Create an additional site for the VLL service, if required. Repeat steps 7 to 38.
- **b** Complete service creation. Go to step 40.

40 Click on the OK button. The VLL Ipipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-9 To create a VLL Cpipe service

VLL Cpipe services are configurable only on the 7710 SR, 7750 SR, 7705 SAR, 7210 SAS-M, and 7450 ESS devices. Consider the following when creating a VLL Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

1 Choose Create→Service→VLL→Cpipe (CEM to CEM) from the 5620 SAM main menu. The VLL Cpipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Cpipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Service Cpipe form closes and the VLL Cpipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Default VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled and the Profile Name parameter is left blank.
- Use Bandwidth-Reserved Paths
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 31.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

6 On the navigation tree, right-click on VLL Cpipe and choose Create Cpipe Site. The Select Network Elements - VLL Cpipe form opens with a list of available sites.

7 Choose a site and click on the OK button. The Select Network Elements - VLL Cpipe form closes and the Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

9 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 10.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 70-13.

c Create a spoke SDP binding for the site. Go to step 15.

d Complete site creation. Go to step 28.

10 On the navigation tree, right-click on Endpoints and choose Create Endpoints. The Endpoint (Create) form opens.

11 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

12 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 10 to 12 for each endpoint in the VLL service.

13 Click on the Apply button.

14 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform steps 4 to 33 of Procedure 70-13.

b Create a spoke SDP binding for the site. Go to step 15.

c Complete site creation. Go to step 29.

15 On the navigation tree, right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

16 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

17 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth

18 Perform one of the following to specify a transport tunnel for the spoke SDP binding:

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto-Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth=“true”/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag “Insufficient Bandwidth To Allocate To SDP Binding” will be raised.

Refer to Chapter 6 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

19 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

20 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab button.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth parameter in step 17.

b Configure the transport tunnel manually.

i Click on the Return tab button.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

21 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

22 Click on the States tab button.

23 Configure the Administrative State parameter.

24 Click on the Pseudowire OAM tab button.

25 Configure the Control Word parameter.

26 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

27 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service navigation tree.

28 Click on the OK button. The Site (Create) form closes and a dialog box appears.

29 Click on the OK button. The VLL Cpipe (Create) form reappears with the new information displayed in the service navigation tree.

30 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 29.

b Complete service creation. Go to step 31.

31 Click on the OK button. The VLL Cpipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-10 To create a 9500 MPR Cpipe service

1 Choose Create→Service→9500 VLL→Cpipe (CEM to CEM/Eth) from the 5620 SAM main menu. The Cpipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Cpipe service. The Select Customer - Cpipe Service form opens.

3 Choose the Default Customer as the customer for the Cpipe service and click on the OK button. The Select Customer - Cpipe Service form closes and the Cpipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Specify VLAN Path
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Click on the Select button to choose a VLAN path to associate with the Cpipe service. The Select VLAN Path - Cpipe Service form opens.

Note — If no VLAN path exists, see Procedure 69-12 for more information about how to create VLAN paths.

6 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Cpipe Service form closes and the Cpipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

7 Configure the parameters:

- Auto-Assign ID
- VLAN ID

The VLAN ID parameter is enabled when the Auto-Assign ID parameter is disabled.

8 Configure the Service Class parameter.

9 If you specified the CEM to Eth option in step 8, configure the parameters:

- EC ID Tx
- Auto-Assign ID
- EC ID Rx
- Auto-Assign ID
- Clock Source
- Mac Address

The VLAN ID parameters are enabled when the associated Auto-Assign ID parameter is disabled.

10 If you specified the SDH to SDH option in step 8, configure the parameters:

- Clock Source
- Jitter Buffer Depth

11 On the navigation tree, right-click on Cpipe Service and choose Create Cpipe Site. The Select Network Elements - Cpipe Service form opens with a list of available 9500 MPR sites.

For information on adding a GNE site to a VLL service, see Procedure 70-12.

12 Choose a site and click on the OK button. The Select Network Elements - Cpipe Service form closes and the Cpipe Site (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

14 On the navigation tree, right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

15 Configure the Name parameter.

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The L2 Access Interface (Create) form closes, and the Cpipe Site (Create) form reappears with the new interface information displayed in the service navigation tree.

21 Repeat steps 14 to 20 if you need to create another L2 access interface for the site in the Cpipe service.

22 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 11 to 21.

b Complete service creation. Go to step 23.

23 Click on the OK button. The VLL Cpipe (Create) form closes.

You can use the service topology maps to view the service. See chapter 5 for more information about service topology maps.

Note — In case of a service creation failure and/or generated NE inconsistencies, see Procedure 37-21.

Procedure 70-11 To fix a failed cross-connection in a 9500 MPR Cpipe

The 5620 SAM may fail to establish one or more cross-connects when you deploy a 9500 MPR Cpipe service, or a cross-connect may fail after the service is created. If you determine that a service is down because of a failed cross-connect, you can try to re-establish the cross-connect.

Note — You must clear deployment errors that are associated with a failed cross-connect before you attempt to re-establish the cross-connect.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria for the service type that you need to find and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a 9500 MPR Cpipe service and click on the Properties button. The Cpipe Service (Edit) form opens with the General tab displayed.

4 Click on the Complete Service button. A dialog box appears.

5 Click on the Yes button.

6 Verify that the cross-connects are operational.

7 Close the Manage Services form.

Procedure 70-12 To configure a GNE site on a VLL service

Use this procedure to add a GNE site and GNE service interfaces to an existing VLL service. This procedure applies to VLL Epipe, Apipe, Fpipe, Ipipe, and Cpipe services. This procedure also applies to 9500 MPR VLL Epipe, Apipe, and Cpipe services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VLL service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on *VLL_type* Service and choose Create GNE Site. The Select Network Elements - *VLL_type* Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

  i Click on the GNE Service Interfaces tab button and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

  ii Configure the parameters:

  - Name
  - Description
  - Type

  iii Click on the Ports tab button and then click on the Select button next to the Interface Index field. The Select Generic NE Interface form appears.

  iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

  v Configure the parameters:

  - Encap Type
  - Outer Encapsulation Value
  - Inner Encapsulation Value

  vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab button to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The *VLL_type* (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The *VLL_type* (Edit) form closes.

You can use the topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 70-13 To create a VLL L2 access interface on a terminating site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL and click on the Properties button. The VLL *VLL_type* (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site on which you want to create a VLL L2 access interface; expand the entries for that site.

For information on adding a GNE service interface to a VLL service, see Procedure 70-12.

5 Right-click on Access Interfaces below the site and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- ATM Connection Type
- MC Ring Node
- Tunnel Fault Notification
- Enable AIS

The ATM Connection Type parameter is configurable only in a VLL Apipe service that has the VC Type parameter set to ATM-cell.

The MC Ring Node parameter is configurable only in a VLL Epipe service.

The Tunnel Fault Notification parameter is configurable on L2 access interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

The Enable AIS parameter is configurable only in a VLL Epipe service where the device has ports configured in access or hybrid mode with Q in Q encapsulation to forward AIS frames generated by a facility tunnel MEP.

7 If you are creating a redundant L2 access interface, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to choose an endpoint for the L2 access interface. The drop-down menu displays the available endpoints.

ii Choose an endpoint from the drop-down menu.

8 Click on the Select button beside the Application Profile parameter. The Application Profile String: - L2 Access Interface form opens.

Note — The Application Profile parameter is configurable only for an Epipe and Ipipe L2 access interface.

9 Choose a profile from the list and click on the OK button. The Application Profile String: - L2 Access Interface form closes and the L2 Access Interface (Create) form is refreshed with the application profile information.

Note — The Application Profile String: - L2 Access Interface form only displays local profiles that are on the node.

10 Associate an AA transit prefix policy with the service object, if required.

- **i** Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.
- **ii** Select a transit IP policy and click on the OK button.

11 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

- **i** Click on the 5670 RAM Parameters tab button.
- **ii** Click on the Reporting tab button.
- **iii** Click on the Create button. The AA Reporting (Create) form opens.
- **iv** Configure the parameters:
  - Customer Name
  - Subscriber Class
  - Total Bandwidth Upstream (Kbps)
  - Class of Service 1 Bandwidth Upstream (Kbps)
  - Class of Service 2 Bandwidth Upstream (Kbps)
  - Class of Service 3 Bandwidth Upstream (Kbps)
  - Class of Service 4 Bandwidth Upstream (Kbps)
  - Subscriber Name
  - Subscriber Type
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
  - Downstream (Kbps)
- **v** Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.
- **vi** Click on the General tab button.

12 Click on the Port tab button.

13 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

14 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

Note — If you choose an Ethernet tunnel endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

15 Perform one of the following:

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

a If you are creating an Epipe or Ipipe L2 access interface, configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- LLF Enabled

  The LLF Enabled parameter is configurable only for Epipe L2 access interfaces on ports with Null encapsulation.

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID check box to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

The Outer Encapsulation Value (VPI) parameter is configurable only when the port encapsulation type is ATM.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

The Inner Encapsulation Value (VCI) parameter is configurable only when the port encapsulation type is ATM.

If you are creating an Epipe and use dot1q or Q in Q encapsulation, then you can enable ingress VLAN translation, if required. Configure the parameters:

- Translation
- Translation ID

b If you are creating an Apipe L2 access interface, configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- Encapsulation Value
- Encapsulation Value
- Encapsulation Value
- LLF Enabled
- Connection Profile ID

The Encapsulation Value parameter and the Encapsulation Value parameter are configurable only when the VC Type parameter is set to ATM-cell in step 4 of Procedure 70-4 and the ATM Connection Type parameter is set to PVT in step 6 of this procedure.

The Encapsulation Value parameter is configurable only when the VC Type parameter is set to ATM-VPC in step 4 of Procedure 70-4.

The LLF Enabled parameter is configurable only for SAPs with “Port” ATM Connection Type and on a clear channel under 4 port OC3-STM1 ASAP MDA.

The Connection Profile ID parameter is configurable only when the Signalling VC Type Override parameter is set to ATM-VCC or None. The Connection Profile ID parameter can only be associated with an Apipe when the VC Type parameter is set to ATM-cell.

c If you are creating an Fpipe L2 access interface, configure the Outer Encapsulation Value parameter.

d If you are creating a CPipe L2 access interface, go to step 18.

16 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

17 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle was selected in step 14, only the Scheduling Class parameter is configurable.

The Fragment Interleave parameter is configurable only in a VLL Epipe or Ipipe service.

18 Assign ingress and egress QoS policies to the interface, if required.

a To configure a 7450 ESS, 7705 SAR, 7710 SR, or 7750 SR, perform the following steps.

Note — Items such as policies, schedulers and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only on Epipe L2 access interfaces.

The Ingress Match QinQ Dot1P parameter is not configurable if the port encapsulation type is ATM or FR.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L2 Access Interface form opens.

iv Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress QoS policy information displayed.

Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

vi Choose an egress QoS policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the egress QoS policy information displayed.

Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 egress interface has the access egress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

vii If you are configuring an L2 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 14 is not an HSMDA port, then go to step 19.

viii Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

ix Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

x Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the L2 Access Interface (Create) form reappears with the WRR policy information displayed.

xi Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xii Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

b To configure a 7210 SAS-D 6F 4T ETR, 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP, perform the following steps.

i Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - L2 Access Interface form opens.

ii Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - L2 Access Interface form closes and the information is displayed.

Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

iii Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst

Note 1 — The Ingress Meter parameter is configurable only during SAP creation on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP. The parameter must be set to true to support H-metering.

Note 2 — On a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP, the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters are configurable only after SAP creation.

19 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 21.

Note 1 — The Schedulers tab is configurable only if a port is assigned to the interface earlier in the procedure.

Note 2 — For the 7210 SAS-X, the port is enabled only when you select the SAP based type in the Egress Scheduler Mode.

20 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 14 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 14 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - L2 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v If you are configuring this interface for an Ipipe service then go to step viii.

vi Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vii Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

viii If the port you selected in step 14 is an HSMDA port, go to step 21.

ix Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L2 Access Interface form opens.

x Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

xi If you are configuring this interface for an Ipipe service then go to step 21.

xii Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xiii Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xiv Go to step 21.

b Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to On.

Note — You cannot specify an access scheduler policy if the port you selected in step 14 is an HSMDA port. Go to step 21.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L2 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

21 Assign ingress and egress ACL filters to the interface, if required.

Note 1 — IPv6 ACL filters are not supported on the 7705 SAR.

Note 2 — ACL filters are not supported for CPipe L2 access interfaces.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - L2 Access Interface form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - L2 Access Interface form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - L2 Access Interface form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - L2 Access Interface form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

22 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - L2 Access Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

v If you are configuring statistics collection for a 7210 SAS-E or 7210 SAS-M, go to step vi. Otherwise, go to step 23.

vi Configure the parameters:

- Enable Egress Packets Forwarding
- Ingress Counter Mode

vii If you are configuring statistics collection for a 7210 SAS-D 6F 4T ETR, go to step viii Otherwise, go to step 23.

viii Configure the parameters:

- Enable Egress Forwarding
- Enable Ingress Forwarding

23 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button in the Time Of Day Suite panel. The Select Time Of Day Suite - L2 Access Interface list form opens.

iii Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface list form closes, and the L2 Access Interface (Create) form reappears with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface. You must disable the Collect Accounting Statistics parameter in step 22.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

24 Configure an Ethernet tunnel.

Note — You can only configure an Ethernet tunnel if you are creating a same-fate SAP or a control/data SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 25.

iii Click on the Create button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

25 If you need to create an Epipe or Ipipe L2 access interface, specify the queue overrides by clicking on the Override Policy Items tab button.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

Set the queue overrides, as described in Procedure 47-44.

26 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button. The ANCP Static Map (Create) form opens.

ii Configure the ANCP String parameter.

iii Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

iv Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

v Click on the OK button. The ANCP Static Map form closes.

27 Associate a MEP to an Epipe or Apipe L2 access interface, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The MEP (Create) form closes.

28 If you are creating an Epipe, Apipe, or Ipipe L2 access interface, specify OAM functionality and assign ingress and egress ATM policies to the interface. Otherwise, go to step 32.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- ATM OAM Terminate

The ATM OAM Terminate parameter is configurable only on Apipe L2 access interfaces. When the VLL access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU, set the ATM OAM Terminate parameter to Up.

The AAL5 Encapsulation parameter is configurable only on Epipe and Ipipe L2 access interfaces.

The ATM OAM Alarm Cell Handling parameter is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-VCC or ATM-VPC, or when the VC Type parameter is set to ATM-cell and the ATM Connection Type parameter is set to PVC. The parameter is configurable on Epipe and Ipipe L2 access interfaces.

The ATM OAM Terminate is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-SDU or ATM-VCC in step 4 of Procedure 70-4.

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the egress ATM policy information displayed.

29 If you are creating an Ipipe L2 access interface, specify Ipipe functionality for the interface. Otherwise, go to step 32.

i Click on the IPIPE tab button.

ii Configure the parameters:

- CE IP Address
- MAC Refresh Interval
- MAC Address
- Use Broadcast MAC Address

The MAC Address parameter, MAC Refresh Interval parameter, and Use Broadcast MAC Address parameters are configurable only when the port encapsulation type is dot1q, Q in Q, or Null.

30 If you are creating an Epipe L2 access interface with CEM encapsulation, specify the CEM functionality for the service. Otherwise, go to step 32.

Note — Consider the following when creating a VLL Epipe L2 access interface with CEM encapsulation:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

i Click on the OK button to close the L2 access interface configuration form. The Site (Create) form reappears.

ii Click on the OK button. The Site (Create) form closes and the VLL Cpipe (Create) form reappears.

iii Click on the Apply button.

iv On the navigation tree, expand the Site object. Click on the SAP object for the L2 access interface that you are creating. The L2 Access Interface (Edit) form opens with the General tab displayed.

v Click on the CEM EPipe tab button.

vi Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- RTP Header
- Report Alarm
- Local ECID
- Remote ECID
- Remote MAC Address

31 If you are creating a Cpipe L2 access interface, specify the CEM functionality for the service. Otherwise, go to step 32.

Note — Consider the following when creating a VLL Cpipe L2 access interface:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

i Click on the OK button to close the L2 access interface configuration form. The Site (Create) form reappears.

ii Click on the OK button. The Site (Create) form closes and the VLL Cpipe (Create) form reappears.

iii Click on the Apply button.

iv On the navigation tree, expand the Site object. Click on the SAP object for the L2 access interface that you are creating. The L2 Access Interface (Edit) form opens with the General tab displayed.

v Click on the CEM CPipe tab button.

vi Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- Packetization Buffer (ms)
- RTP Header
- Report Alarm

32 Click on the OK button. A dialog box appears.

33 Click on the OK button. The L2 Access Interface (Create) form closes, and the Site (Create) form reappears with the new interface information displayed in the service navigation tree.

Repeat steps 5 to 33 to create another L2 access interface for the site in the VLL service.

Note 1 — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces must be on LAGs that participate in the MC LAG. See chapter 43 for information about MC LAGs.

Note 2 — If you are creating the L2 access interface during service creation, return to the appropriate VLL service creation procedure:

- For Epipes, go to step 18 of Procedure 70-1.
- For Apipes, go to step 14 of Procedure 70-4.
- For Fpipes, go to step 14 of Procedure 70-6.
- For Ipipes, go to step 16 of Procedure 70-8.
- For Cpipes, go to step 14 of Procedure 70-9.

Procedure 70-14 To create a SAP aggregation group

Perform this procedure to create a SAP aggregation group on a 7705 SAR Apipe service.

Note — SAP aggregation groups can be created only on Apipe services that are configured with the ATM VCC or ATM N:1-N>1 VC Type option. See Procedure 70-4 for more information about configuring the VC type.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button.

3 From the list, choose an Apipe service with at least one 7705 SAR site and click on the Properties button. The Apipe Service (Edit) form opens with the General tab displayed.

4 From the component tree, expand to the site level and click on a 7705 SAR site. The Apipe Site (Edit) form opens with the General tab displayed.

5 Click on the Aggregation Group tab button.

6 Click on the Create button. The SAP Aggregation Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Aggregation Group

8 Click on the QoS tab button.

9 Specify an ingress policy for the SAP aggregation group:

   i Click on the Select button in the Ingress Policy panel. The Select Ingress Policy - SAP Aggregation Group form opens.

   ii Configure the filter criteria, if required, and click on the Search button.

   iii Choose an ingress policy and click on the OK button. The Select Ingress Policy - SAP Aggregation Group form closes.

10 Specify an egress policy for the SAP aggregation group:

   i Click on the Select button in the Egress Policy panel. The Select Egress Policy - SAP Aggregation Group form opens.

   ii Configure the filter criteria, if required, and click on the Search button.

   iii Choose an egress policy and click on the OK button. The Select Egress Policy - SAP Aggregation Group form closes.

11 Click on the Accounting tab button.

12 Specify an accounting policy for the SAP aggregation group:

   i Click on the Select button in the Accounting Policy panel. The Select Accounting Policy - SAP Aggregation Group form opens.

   ii Configure the filter criteria, if required, and click on the Search button.

   iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - SAP Aggregation Group form closes.

13 Click on the OK button. The SAP Aggregation Group (Create) form closes.

14 From the component tree, expand the entries of the 7705 SAR site.

15 Right-click on Access Interfaces under the entry and choose Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

16 Configure the parameters:

   - Description
   - Administrative State

17 Click on the Select button in the Aggregation Group panel and choose the SAP aggregation group that you created.

Note — The QoS and Accounting tab buttons are dimmed when an L2 access interface is assigned to a SAP aggregation group. The QoS and accounting policies that are assigned to the SAP aggregation group are automatically assigned to all of the SAPs in the group.

18 Click on the Port tab button.

19 Specify a terminating port for the L2 access interface:

i Click on the Select button in the Termination Port panel. The Select Terminating Port - L2 Access Interface form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a port from the list and click on the OK button. The Select Terminating Port - L2 Access Interface form closes.

20 Configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

21 Click on the ATM tab button.

22 Configure the parameters:

- ATM OAM Alarm Cell Handling
- Subscriber Vlan
- Translated VPI
- Translated VCI

23 Assign an Ingress ATM Policy to the L2 access interface:

i Click on the Select button in the Ingress ATM Policy panel. The Select Ingress ATM Policy - ATM Configuration form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a policy from the list and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes.

24 Assign an Egress ATM Policy to the L2 access interface:

i Click on the Select button in the Egress ATM Policy panel. The Select Egress ATM Policy - ATM Configuration form opens.

ii Configure the filter criteria, if required, and click on the Search button.

iii Choose a policy from the list and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes.

25 Click on the OK button. The L2 Access Interface (Create) form closes.

26 Repeat steps 15 to 25 to create more SAPs, as required.

Note 1 — A SAP aggregation group can contain up to 16 SAPs.

Note 2 — If you are creating the SAP aggregation group during service creation, return to step 15 of Procedure 70-4.

27 Close all forms.

Procedure 70-15 To create an HSDPA resiliency configuration

See “HSDPA Offload Resiliency” in section 70.1 for information about HSDPA resiliency.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Click on the Create button. The HSDPA Resiliency (Create) form opens.

3 Configure the parameters:

- Description
- Administrative State

4 Click the Select button beside the Name parameter in the Site panel. The Select Site - HSDPA Resiliency form opens. Only sites utilizing a 7705 SAR chassis are displayed.

5 Choose a site and click on the OK button. The Select Site - HSDPA Resiliency form closes and the HSDPA Resiliency (Create) form is displayed with your site choice shown in the Name parameter field.

6 Click the Select button beside the Name parameter in the Primary Service panel. The Select Primary Service - HSDPA Resiliency form opens with a list of services.

Note — The Select Primary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 70-4 to create the required service before configuring HSDPA Resiliency.

7 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the primary service information.

8 Click the Select button beside the Name parameter in the Secondary Service panel. The Select Secondary Service - HSDPA Resiliency form opens with a list of services.

Note — The Select Secondary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 70-4 to create the required service before configuring HSDPA Resiliency.

9 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the secondary service information.

10 Click on the OK button. The HSDPA Resiliency (Create) form closes.

11 Perform one of the following:

a Perform Procedure 70-16 to turn up or manually operate an HSDPA resiliency configuration.

b Close the HSDPA Resiliency Manager form.

Procedure 70-16 To activate and manually operate an HSDPA resiliency configuration

See section "HSDPA Offload Resiliency" for a detailed description of this feature.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Choose the required HSDPA resiliency configuration from the displayed list and click the Properties button. The HSDPA Resiliency (Edit) form opens with the properties of the configuration displayed on the General tab.

The Active Service field displays whether the Primary or Secondary Service is active. When you initially want to turn up a resiliency configuration, typically Primary is displayed.

3 Set the Administrative State parameter to Disabled. Activity for the resiliency configuration can only be manually switched from this form when this parameter is set to Disabled.

4 Perform one of the following:

a Set the Administrative State parameter to Enabled. Activity automatically switches between the primary and secondary services as required when this parameter is enabled.

b Click on the Turn Up button to manually activate the HSDPA resiliency configuration. Do this if the Administrative State parameter is not enabled.

c If the Primary Service is currently active, you can click on the Force Secondary Service Active button. This manually forces the configuration to the Secondary Service (if up), regardless of state of damping timer. The Active Service field displays Secondary if the switchover is successful.

d If the Secondary Service is currently active, you can click on the Force Primary Service Active button. This manually forces the configuration to the Primary Service (if up), regardless of state of damping timer. The Active Service field displays Primary if the switchover is successful.

e Click on the Shut Down button to de-activate the HSDPA resiliency configuration.

f Click on the Faults tab to view and address alarms related to the configuration.

5 Click on the OK button. The HSDPA Resiliency (Edit) form closes.

6 Close the HSDPA Resiliency Manager form.

Procedure 70-17 To run an OAM validation test for a VLL service

An OAM validator test suite must be created for the tested entity. See chapter 78 for more information about how to create a validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens with the General tab displayed.

4 Click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

- **i** Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.
- **ii** Configure the filter criteria. A list of OAM validator test suites appears.
- **iii** Choose an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button. The Test Suite tab is displayed.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VLL *Type_of_VLL* (Edit) form.

15 Close the Manage Services form.

Procedure 70-18 To view the service topology associated with a VLL service

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.
3. Choose a VLL service and click on the Topology View button. A Topology View dialog box appears.
4. Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

   See chapter 5 for more information about service topology views.

Procedure 70-19 To view the VLL service operational status

The Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
3. Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.
4. View the Operational State and State Cause indicators. When the Operational State is Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.
5. Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.
6. Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.
7. Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.
8. Close the VLL *Type_of_VLL* (Edit) form.
9. Click on the Close button to close the Manage Services form.

Procedure 70-20 To view the peer status information associated with the VLL service

You can view peer status faults in the peer PE SAP and service tunnel in the Peer State Cause panel of the Spoke SDP Binding form.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 Click on the Spoke SDP Binding tab button.

5 Choose an entry and click on the Properties button. The Spoke SDP Binding (Edit) form opens.

6 Click on the States tab button.

7 View the peer status information in the Peer State Cause panel. When the service tunnel or peer SAP is down or partially down, a check mark beside the appropriate Peer State Cause indicator identifies the type of associated service fault.

8 Click on the Cancel button to close the Spoke SDP Binding (Edit) form.

Procedure 70-21 To modify a VLL service

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL service and click on the Properties button. The *VLL_type* Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

Note 1 — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

Note 2 — Some service element do not apply to all VLL services.

- Sites tab — lists the sites that are included in the service
- Endpoints tab — lists the service endpoints
- L2 Access Interfaces tab — lists the L2 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- VLAN Path Instance - list VLAN path instances associated with a 9500 MPR service
- Template tab — displays the template used to create the service, if applicable.
- Tests tab
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service as required.

To configure items on the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The *VLL_type* Service (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 70-22 To modify a VLL service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 17.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the option allowing you to create a new site. This may be an Epipe, Cpipe, Ipipe, Apipe, or Fpipe site, depending on what type of VLL service you are modifying.

The Select Network Elements form appears.

5 Choose one or more sites to add to the service and click OK. The Site (Create) form for the new site is displayed. If you selected more than one site, the Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The Site (Create) (or Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedures 70-1 through 70-10 for detailed site configuration information for the various types of VLL services.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

Creating site components

9 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- Endpoint. Go to step 10.
- L2 Access Interface. Go to step 13.

10 If you choose to create an Endpoint, then the Endpoint (Create) form is displayed.

11 Configure the Name parameter for the endpoint.

Refer to Procedures 70-1 through 70-9 and 70-13 for detailed information on further configuring the endpoint, if required.

12 Click OK. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

13 If you choose to create an L2 Access Interface, then the L2 Access Interface (Create) form is displayed.

14 Click on the Port tab and assign a port to the interface.

Refer to Procedures 70-1 through 70-10 and 70-13 for detailed information on further configuring the interface, as required.

15 Click OK. L2 Access Interface (Create) form closes.

16 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

Creating spoke SDP bindings

17 Choose the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

18 Choose Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

19 Enable the Auto-Select Transport Tunnel parameter.

20 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedures 70-1 through 70-9 for more detailed information on creating and configuring spoke SDP bindings for the various types of VLL services, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

21 Assuming that the spoke SDP binding was successfully created in step 20, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

22 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

23 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

24 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

25 Close the Service Topology form.

26 Close the Manage Services form.

Procedure 70-23 To delete a VLL service

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This message is dynamic based on the priority of the service. Perform one of the following:

  a For services with a low priority, go to Step 5.

  b For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.

  c For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

71 — VPLS management

71.1 VPLS management overview

VPLS is a class of virtual private network multipoint L2 service that allows multiple customer sites to be connected in a single bridged domain contained within the service provider-managed IP/MPLS network. Customer sites in the VPLS appear to be on the same LAN, even if the sites are geographically dispersed.

VPLS offers the following advantages:

- Ethernet interfaces on the host access side simplify provisioning.
- All routers in the VPLS are part of the same LAN, which simplifies IP addressing and allows customers to control and simplify their routing strategies.
- VPLS is protocol independent, which means there is no L2 protocol conversion between LAN and WAN technologies.

A VPLS can span a single site or multiple sites. A VPLS that spans a single site is called a local VPLS. In a local VPLS, customer data enters the service through multiple access interfaces on a single PE device. No circuit provisioning is required for the local VPLS.

A VPLS that spans multiple sites is called a distributed VPLS. In a distributed VPLS, customer data enters the service using two or more interfaces on different PE devices. The VPLS is transported by service circuits over an IP/MPLS provider core network carried by service tunnels. Service tunnels are created using GRE or MPLS LSPs.

You can use HVPLS to eliminate the need for a full mesh of virtual circuits between devices in the VPLS. See “HVPLS” in this section for more information.

The 5620 SAM supports end-to-end VPLS configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

You can run the OAM Validation test suite for the service by clicking on the More Actions > Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays detailed information about the OAM test result. OAM validation tests are not supported for HVPLS. See chapter 78 for more information about how to configure OAM validation test suites.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. Alarms can be viewed on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 76 for more information about the hierarchical organization of composite services.

Common to all services, such as VPLS, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces and circuits, when the service is configured or modified. The following policies are common to all services:

- QoS policies to define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy Manager and the Access Egress Policy Manager.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy and HSMDA Scheduler Policy forms.
- Filter policies to control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter Manager and the ACL MAC Filter Manager.
- Accounting policies to count the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy Manager.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 46 for more information about policies.

Packets that arrive at an edge device are associated with a VPLS based on the access interface on which they arrive. An access interface is uniquely identified using the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

If there are service issues, the service provider can use OAM tools to troubleshoot service and network transport issues, and ensure problems are handled properly through the physical and logical network. See chapter 38 for more information.

To provide a VPLS over an MPLS infrastructure, the device is configured to provide bridging and replication for each VPLS. The routers that are part of the VPLS are connected by MPLS LSPs. Multiple VPLS can use the same set of service tunnels. Multiple service tunnels can rely on multiple LSPs. The signaling is specified in sets of ingress and egress VC labels for each VPLS.

The following additional features are configured for the VPLS:

- MAC learning for the access ports and tunnels, including filtering based on MAC addresses on a per SAP basis
- MAC learning protection on SAPs to prevent DoS attacks from sourcing
- rate limiting of broadcast, destination unknown, and multicast traffic on a per access port basis
- FIB for each VPLS, including FIB size limits, static MAC addresses, alarms, and discarding unknown locations
- optional support for spanning tree for loop detection
- GSMP for each VPLS
- L2 management interfaces for each VPLS

HVPLS

A hierarchical VPLS is created by enhancing the VPLS core mesh with a spoke SDP binding that is connected to another site in the same VPLS, a site in another VPLS, or a VLL site.

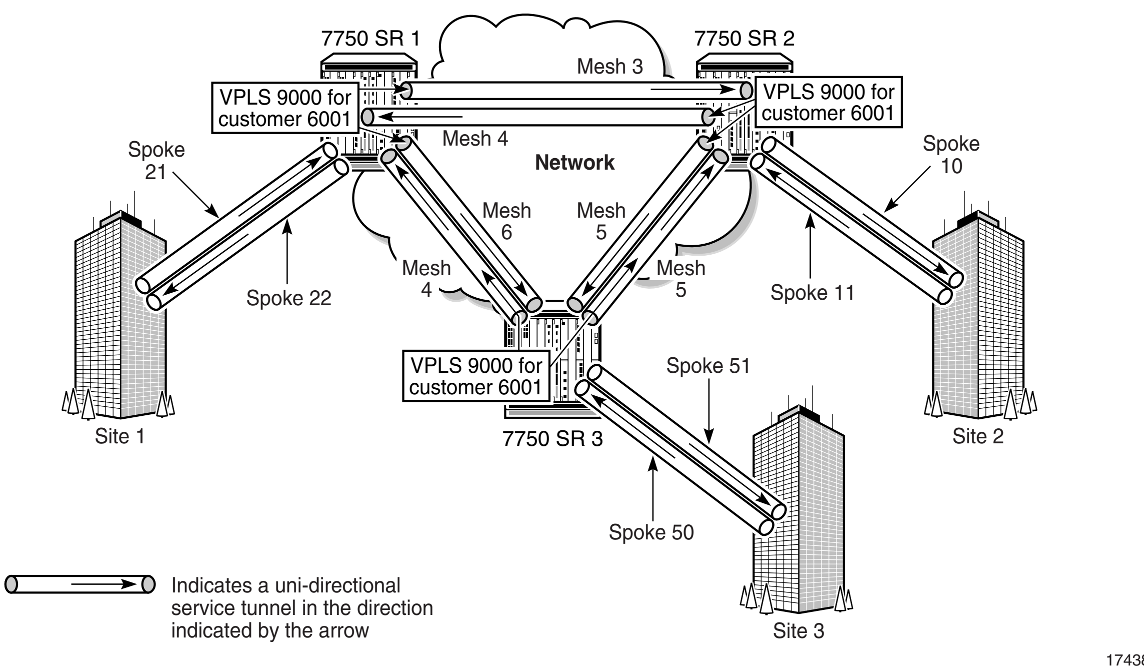
HVPLS offers the following advantages:

- reduces the complexity of mesh configuration
- decreases the amount of signaling of routes between devices

When traffic arrives at an access-spoke circuit, it acts like a bridge port where flooded traffic received on the access spoke is replicated to all other spokes, meshes, or SAPs but it is not transmitted on the port where it is received.

Figure 71-1 shows a sample HVPLS with a mesh and spoke configuration. Spokes 50 and 51 are unidirectional access-spoke circuits bound to service tunnels. The access-spoke circuits exist within the context of a VLL service or VPLS that is interconnected to the original, fully meshed VPLS. Alternatively, the access-spoke circuit can provide interconnectivity to a service site.

Figure 71-1 HVPLS configuration



The 5620 SAM supports the following HVPLS interconnectivity using spoke SDPs:

- VPLS to VPLS
- intra-VPLS
- VPLS to VLL

MVPLS

VPLS topology loops can occur if either of the following is true:

- Two VPLS are connected by redundant spoke SDPs.
- A CE NE is connected to a VPLS with redundant L2 access interfaces.

To remove topology loops, RSTP must be enabled on the redundant spoke SDPs or L2 access interfaces to block some of them from passing traffic. This requires the creation of an MVPLS.

MSTP is an extension of RSTP which allows VLANs to be grouped into spanning tree instances. Each instance has an independent spanning tree topology. MSTP can be run in an MVPLS to provide multiple forwarding paths for data traffic, which allows load balancing and reduces the number of spanning tree instances required to support a large number of VLANs. An MST region comprises a set of interconnected switches that have the same MST configuration. Each region can be configured with up to 16 MST instances. The instance with ID 0 is an internal spanning tree that runs an MST region and sends and receives BPDUs. All other spanning tree instance information is encapsulated within MSTP BPDUs.

An MVPLS is created to run RSTP or MSTP and manage traffic on the associated VPLS. An MVPLS contains sites, spoke SDP bindings, mesh SDP bindings, and L2 access interfaces. The MVPLS spoke SDP bindings and L2 access interfaces are configured to manage the associated VPLS spoke SDP bindings and L2 access interfaces.

In the case of spoke redundancy, the MVPLS runs RSTP on the redundant spoke SDPs and associates the resultant traffic-blocking actions with all VPLS that use the same spoke SDPs.

MVPLS traffic blocking can also be used on the access side to manage redundant L2 access interface connections. A VLAN ID range is specified for each MVPLS L2 access interface which identifies the VC IDs of the managed VPLS L2 access interfaces.

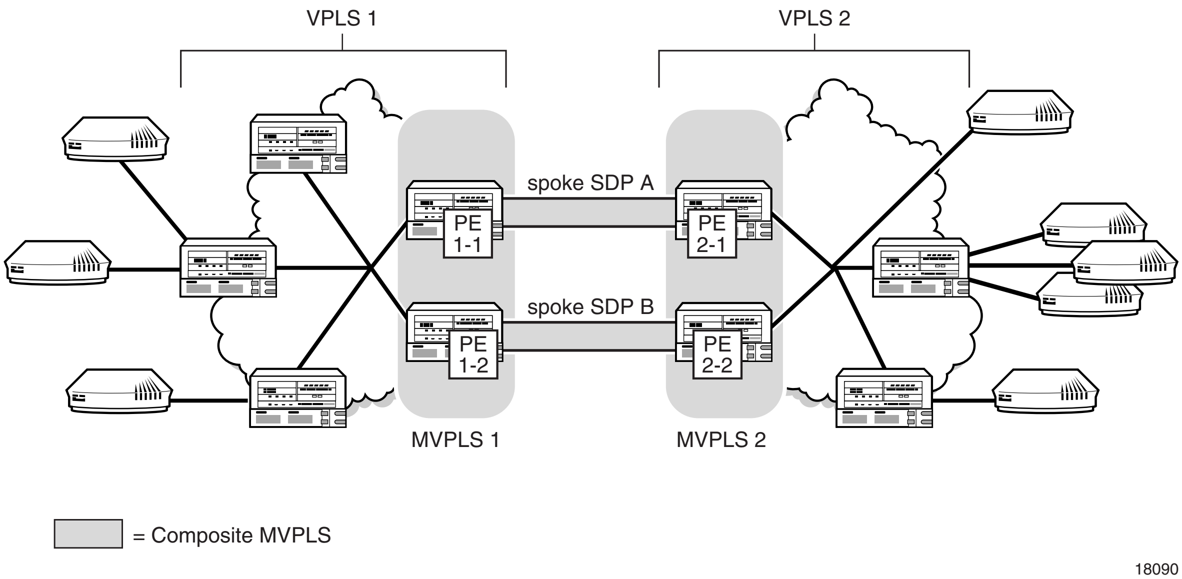
RSTP is enabled by default on an MVPLS. When the Admin state of an MVPLS is down, all managed L2 access interfaces and spoke SDPs in the associated VPLS are disabled. However, if the Admin state of individual L2 access interfaces or spoke SDPs of an MVPLS are down, then the managed VPLS L2 access interfaces or spoke SDPs are not affected by traffic blocking.

A common MVPLS situation occurs when two VPLS are connected by redundant spoke SDPs. If traffic is not blocked on one of the redundant spoke SDPs, then a loop results. To remove the loop, RSTP must be run on the spoke SDPs that form the loop to block one of the redundant spoke SDPs. Blocking is accomplished by creating an MVPLS on each side of the redundant spoke SDPs and creating a composite MVPLS to connect the MVPLS.

Another common MVPLS situation occurs when an access switch with many VLANs is redundantly connected to two other bridges, on which each uplink carries half the VLANs. MSTP allows you to build multiple spanning trees over VLAN trunks and to group and associate the VLANs to spanning tree instances, each with a different port instance cost and port instance priority.

Figure 71-2 shows an example of a composite MVPLS that is composed of MVPLS 1, MVPLS 2, and spoke SDPs.

Figure 71-2 Composite MVPLS



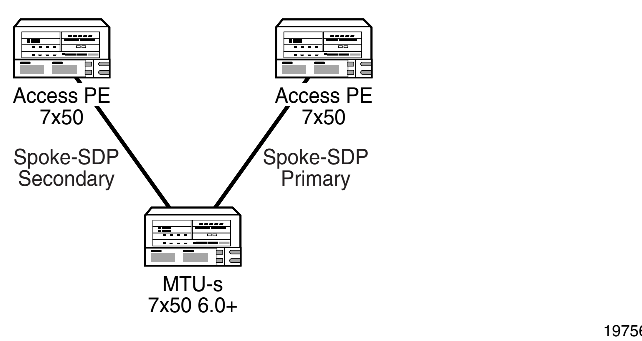
Another scenario occurs when multiple L2 access interfaces from a VPLS are connected to the same customer edge equipment. In this case, a single MVPLS must be created with L2 access interfaces defined to manage the traffic on the associated VPLS redundant L2 access interfaces.

Dual homing for VPLS

A VPLS can be configured for dual homing through the use of redundant spoke SDPs. 5620 SAM handles the redundant spoke SDPs by grouping them together to form an endpoint object. The redundant spoke SDPs provide active and standby pseudowires for the service. This spoke SDP access arrangement allows data flow control and management support without requiring STP, which cannot be enabled on a spoke SDP binding that is under an endpoint. For VPLS, you can associate only spoke SDP bindings with an endpoint, and each endpoint can be associated with a maximum of two spoke SDP bindings.

Figure 71-3 shows a simple dual homing configuration.

Figure 71-3 MTU redundant access to VPLS



VPLS dual homing provides the ability to have an NE deployed as an MTU-s with links to multiple PE NEs without requiring an MVPLS.

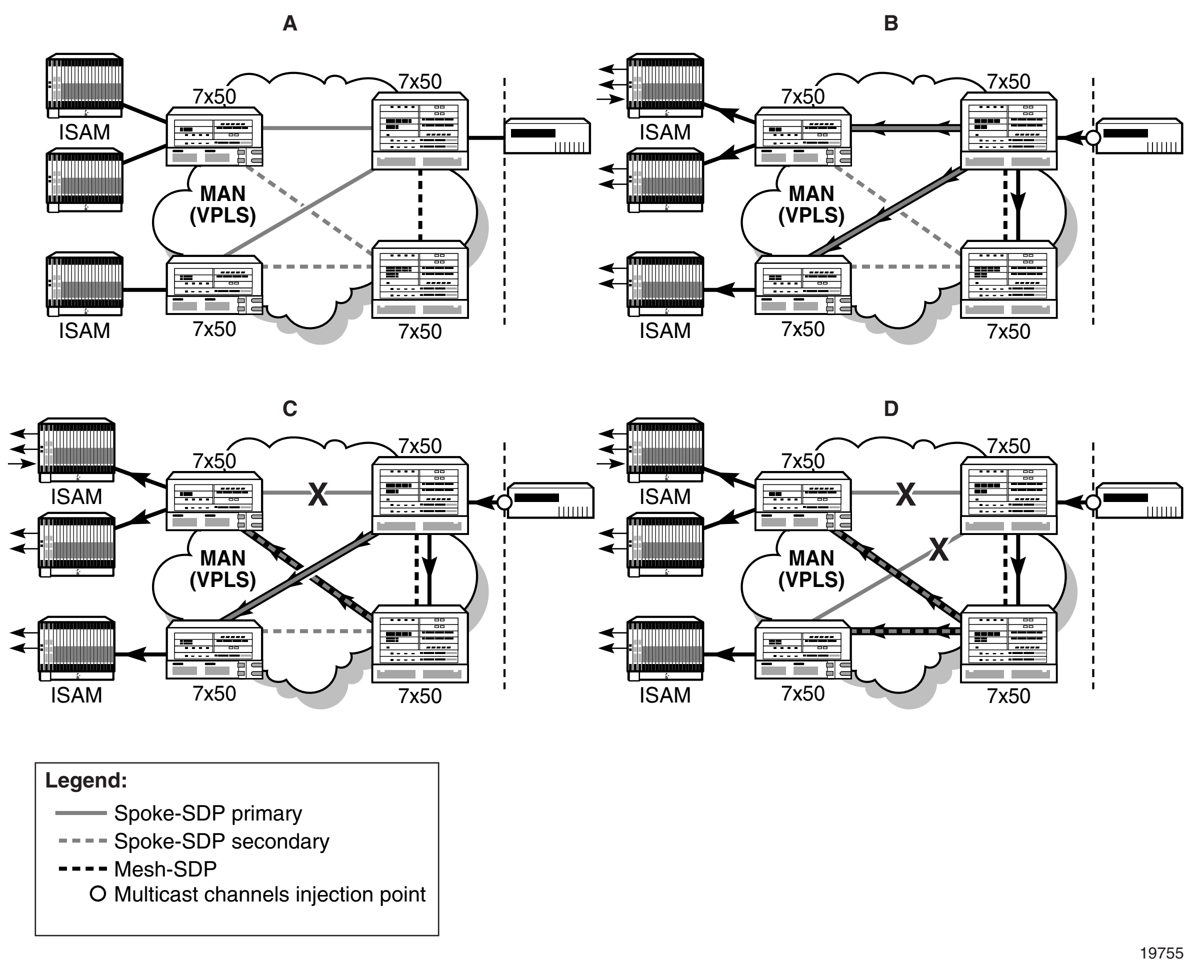
Note 1 — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 45 for more information.

Note 2 — You cannot create an endpoint in an MVPLS.

In this example, the MTU-s has spoke SDPs to two PE devices. One is designated as the primary spoke and the other as the secondary, or standby spoke, based on a precedence value specified for each spoke. The standby spoke is in a blocking state when the primary spoke is available. If the primary spoke becomes unavailable, the MTU-s immediately switches the traffic to the standby spoke. You can configure the service to revert back to the original configuration, after a specified delay, when the primary spoke is again available. Forced manual switchover is also supported.

You can configure a MAC flush to speed the convergence during a switchover. The PE devices that receive the MAC flush remove each MAC address that is associated with the affected VPLS instance and forward the MAC flush to the other PE devices in the VPLS. Figure 71-4 shows a dual-homed VPLS for BTV distribution.

Figure 71-4 BTV distribution in redundant VPLS architecture

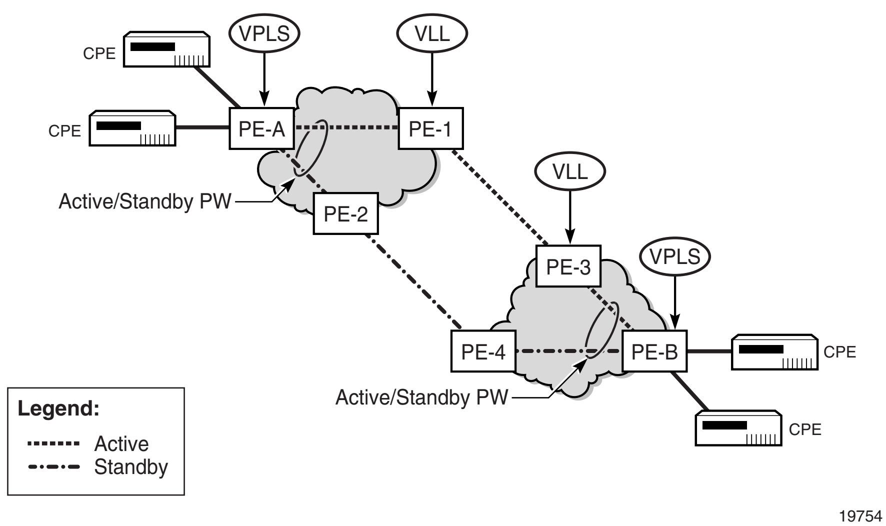


In the nominal operating mode shown in panel A, the edge router (grey icon) has been configured to statically join all multicast channels and inject them into the aggregation network. The access layer 7x50 unit (directly connected to ISAM) is dual-homed into two aggregation layer 7x50s edge routers (larger icons) using primary and secondary spoke SDPs. A mesh SDP interconnects both aggregation nodes. Injected BTV traffic from the edge router is broadcast on the primary spoke SDPs to the connected MTU devices (panel B).

A copy of the channels is also sent on the mesh SDP to the peer aggregation node, which also replicates the traffic to the connected spoke SDPs (aggregation layer nodes are not aware of primary/secondary spoke selection done by the MTU layer devices). The MTUs only receive traffic from the primary spoke SDP. Traffic received on the secondary spoke SDP is blocked. In the event of a link failure (panel C) or MDA failure (panel D), the MTU switches over to the secondary spoke SDP and immediately start receiving traffic from it instead of the primary spoke SDP.

Composite services also support VPLS with redundant spoke SDP bindings to VLL services. Figure 71-5 shows a VPLS and VLL combination example that provides an E2E redundant path.

Figure 71-5 VPLS and VLL combination to provide E2E redundant path



Provider Backbone Bridging in VPLS

Provider Backbone Bridging (PBB) is a technology configuration employed in next-generation networks that utilize carrier-grade Ethernet as the transport architecture. It addresses the potentially enormous increase in MAC addresses stored in the router lookup databases by encapsulating the customer frame in a Provider Ethernet header. The Customer MAC address (C-MAC) is then only dealt with by lower tier (or satellite) H-VPLS PEs. The core H-VPLS PEs only need to handle the backbone provider's MAC addresses (B-MAC), which are substantially less in number. For this reason, the technique is also referred to as MAC-in-MAC encapsulation.

IEEE 802.1ah defines an architecture and bridge protocols for interconnection of multiple Provider Bridge Networks (PBNs). PBB is defined in IEEE as a connectionless technology based on multipoint VLAN tunnels. MSTP is used as the core control plane for loop avoidance and load balancing. As a result, the coverage of the solution is limited by STP scale in the core of large service provider networks.

A Provider Backbone Bridged Network is a Virtual Bridged Local Area Network that comprises Backbone Edge Bridges (BEBs) and Backbone Core Bridges (BCBs) under the administrative control of a single backbone provider. Each BEB provides interfaces that encapsulate or verify the encapsulation of customer frames, and then relay those frames across the backbone. The term that the customer used may also mean a provider who is purchasing a service from another provider and using either a PBN or PBBN internally.

Backbone VLANs are used to create multipoint trunks in the backbone. The B-VLAN determines the route the frames take and limits broadcasting within the backbone. The B-TAG is added to the frame at the Customer Backbone Port (CBP). The selection of B-VLAN used to form the B-TAG is determined by the configuration of the CBP service instance table. This table maps ISIDs to B-VIDs and is created as part of service provisioning.

Backbone VLAN Connectivity

The backbone provider can use and configure MSTP to provide a number of independent spanning tree active topologies and can assign each B-VLAN to one of these active topologies to best use the resources in the network. MVRP, running in the context of each spanning tree active topology, configures the extent of each B-VLAN to the subset of that active topology necessary to support connectivity between the customer points of attachment to the instance of MAC service provided, and can reconfigure that connectivity as required if the spanning tree active topology changes. The operation of MSTP within a backbone provider's network is independent of the operation of any spanning tree protocol within attached provider or customer networks. This is achieved by removing all MSTP BPDUs received or to be transmitted at the service access interfaces. The operation of MVRP within a PBBN is independent of the operation of any configuration protocol within attached customer networks.

SR PBB implementation

The IEEE PBB model is organized around a B-component handling the provider backbone layer and an I-component concerned with the mapping of Customer/Provider Bridge (Q in Q) domain (that is, MACs, and VLANs) to the provider backbone (that is, B-MACs, and B-VLANs). The I-component contains the boundary between the customer and backbone MAC domains. PBB encapsulates the customer payload in a provider backbone Ethernet header, which allows the C-MACs to be hidden from the core PEs. A special Group MAC is used for the Backbone Destination MAC when the customer frame type is either unicast, multicast, broadcast, or unknown.

The SR PBB solution can be summarized as follows:

- Two VPLS variants are employed, namely B-VPLS and I-VPLS, functioning as the B-type BEB, and the I-type BEB respectively. A B-VPLS instance (a service instance within a service router) and its corresponding I-VPLS instances must be co-located in a service router. From a network-wide perspective, a B-VPLS comprises multiple Backbone Virtual Switch Instances (B-VSIs).

  Note — For the description in this section and in the procedures in this chapter, B-VSI is used for a single B-type BEB instance, and is referred to as a B-Site. Similarly, I-VSI is used for a single I-type BEB instance, and is referred to as an I-Site.

- mB-VPLS and mI-VPLS are also available to provide loop avoidance for B- and I-VPLS in the same way as m-VPLS and regular VPLSs operate.
- A 5620 SAM VPLS can include regular sites and either B-Sites or I-Sites. The service should not contain both B-Sites and I-Sites. When a VPLS has at least one B-Site it becomes a B-VPLS. When a VPLS has at least one I-Site, it becomes an I-VPLS.

  Note — Regular sites, B-Sites, and I-Sites cannot change their type after they are created.

- An I-Site can be bound to one B-Site, but a B-Site can be used by multiple I-VPLSs.
- PBB is configurable on a Release 6.4.2 or later OS 9700E or OS 9800E, and on the 7450 ESS, 7710 SR, and 7750 SR.

B-VPLS and I-VPLS instances

PBB processing may be seen as a chain of two linked VPLS contexts, namely B-VPLS and I-VPLS. Their characteristics are summarized in the sections that follow.

I-VPLS

I-VPLS is the abbreviated form for Service Instance ID (ISID) VPLS. An I-VPLS instance on a service site is referred to as an I-Site.

The following are I-VPLS and I-Site characteristics:

- An I-Site operates using customer addressing and maps the C-MACs to B-MACs.
- You can select one B-Site to associate with an I-Site; the B-Site must be on the same PE NE as the I-Site.
- I-Sites support only spoke SDP bindings and not mesh SDP bindings.
- An I-Site L2 access interface, or I-SAP, can co-exist on a port with regular L2 access interfaces or subscriber management M-L2 access interfaces. The existing port encapsulation is supported. An encapsulation tag that is used for service selection on an I-SAP is removed before the PBB encapsulation is added. The appropriate encapsulation tags are added at the remote PBB PE when sending the packet out on the egress access interface.

- An I-Site can be connected to one or more regular VPLS sites. A regular (network level) VPLS can have a mix of regular sites and I-Sites. The I-Sites of such services are responsible for the mapping of C-MACs to B-MACs. The regular sites of the service function as normal (bridge).
- ISID is a 24-bit field that carries the service instance identifier associated with this frame. It is used at the destination PE as a demultiplexer field, a function similar to a VC label. Default to service ID only works if the service ID is within the ISID range. For a service with service ID larger than 16 777 215, the ISID value must be specified.
- The ISID must be unique on one router.
- The Provider MSTP support in an M-VPLS is in the I-VPLS space.
- The I-Site MTU must be at least 18 bytes smaller than the B-Site MTU to which it is bound.
- If a VPLS has an attached I-Site, the Include I-Site(s) indicator on the General tab of the VPLS configuration form is selected.
- IGMP snooping can be configured for I-Sites and I-L2 Access Interfaces.

Backbone-VPLS (B-VPLS)

Multiple L2 services can use a single B-VPLS. Ordinarily, a pair of SDP bindings (in opposite directions) provide either point-to-point connection between two sites of a service (as SDP bindings) or between different services (as a service connector). However, a B-VPLS provides a multipoint connection between sites of a service or for multiple services.

The following are properties and characteristics of a B-VPLS and B-Sites:

- The B-VPLS operates using the provider or backbone addressing (B-MACs).
- The B-VPLS provides backbone tunneling for one or multiple I-VPLSs.
- The B-VPLS accepts mesh or spoke SDP bindings, thereby providing both routing and MAC hiding using PBB/PW encapsulation.
- The B-VPLS accepts access interfaces using PBB encapsulation for tunneling through an Ethernet-only network.
- A regular (network level) VPLS can have a mix of regular sites and B-Sites to function as a B-VPLS (that is, operating using B-MACs).
- The backbone’s Source MAC address can be configured on a B-Site. All the I-Sites provisioned under this B-Site shares the provisioned values. By default, this is a loopback chassis MAC address. It must be a unicast MAC address.
- A B-Site site can not be deleted until all its I-Site associations are removed.
- A B-Site can have both spoke and mesh SDP bindings and only an MPLS type of tunnel can be used (including LDP SDP). This also applies for a regular pseudowire, where the outgoing PBB frame on a B-SDP (that is, a B-PW) contains a B-VID qtag only if the PW type is Ethernet VLAN. Alternatively, if the pseudowire type is Ethernet, the B-VID qtag is stripped before the frame goes out.

- Only Null, dot1q, and Q in Q encapsulation types can be used by a B-Site L2 access interface. These access interfaces must use PBB encapsulation and have the following properties:
  - Ethernet dot1q is applicable to the bulk of PBB use cases, such as one B-VID.
  - Ethernet Null is supported for direct connection between neighboring I-VPLS, for example, when no B-VID is required and all traffic is sent to or from local I-VPLS.
  - There is no requirement for a PBB SAP type for PBB on the B-VPLS SAPs. Only the B-VID is used for tunnel delimitation on the port.
  - The default access interface type is blocked for the B-L2 access interface.
  - The following rules apply to the SAP processing of PBB frames:

    > For transit frames (frames not destined to a local MAC), there is no need to process the I-tag component of the PBB frames. Regular Ethernet SAP processing is applied to the backbone header (B-MACs and B-VID).

    > If a local I-VPLS instance is associated with the B-VPLS, then local frames (frames originated or terminated on local I-VPLSs) are PBB encapsulated and de-encapsulated using the pbb-etype provisioned under:

    related port->I-VPLS->root pbb component

    (listed in decreasing order of precedence, where the related port is highest in the order).
- If a VPLS has an attached B-Site, the Include B-Site(s) indicator on the General tab of the VPLS configuration form is selected

Service topology map views

Service and composite service topology maps support PBB.

The service map shows different types of sites with various icons for I-Sites, B-Sites, and Epipe PBB sites. With an I-VPLS bound to B-VPLS, the map shows the PBB backbone network as a cloud. The bindings between I-VPLS and B-VPLS are shown as a binding link.

MRP and MMRP support

The Multiple Registration Protocol allows participants in an MRP application to register Group MAC addresses with other participants in a Bridged LAN. An MRP participant may transmit and receive MRP PDUs. For the PBB implementation, the MRP parameters can be configured at the service site level, on the access interface, or the SDP binding.

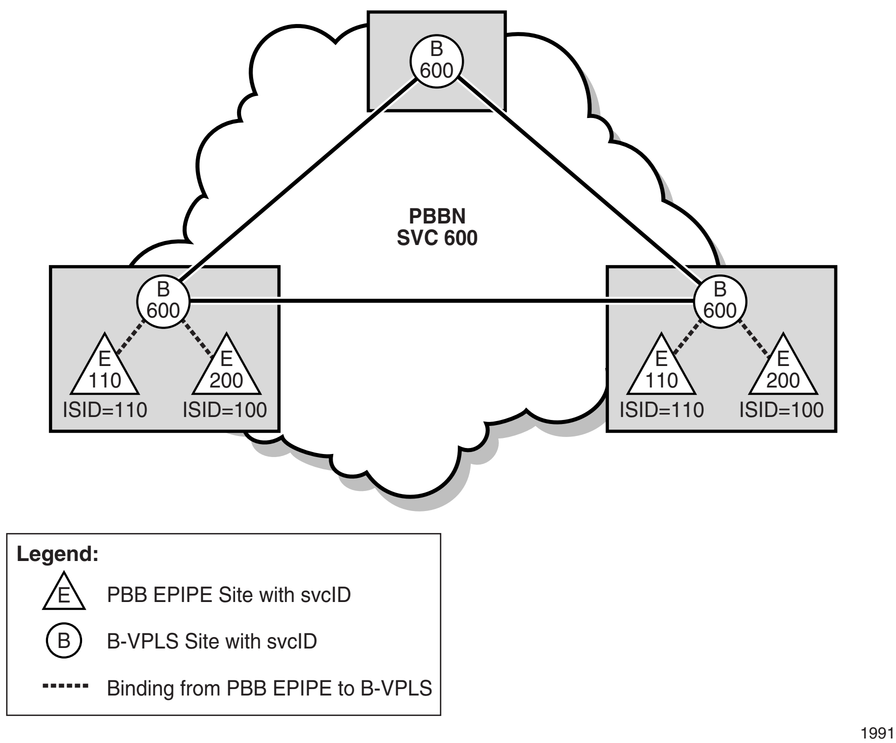
If MRP is enabled on the node, 5620 SAM's MMRP application automatically advertises the presence of the Group B-MAC address on the active B-VPLS virtual links (that is, on the B-Site spoke bindings or the B-L2 access interfaces). You can view the MMRP entries advertised and/or received on the Forwarding Control>MMRP Entries tabs of the B-Site spoke bindings or the B-L2 access interfaces. All the MMRP entries may also be viewed together at the I-Site level.

Epipe service with PBB

A PBB tunnel may be linked to an Epipe and to a B-VPLS. MAC switching and learning is not required for the point-to-point service, since all packets ingressing the Epipe access interface are PBB encapsulated and then forwarded to the PBB tunnel for the backbone destination MAC address. Similarly, all the packets ingressing the B-VPLS and destined for the ISID are PBB de-encapsulated and then forwarded to the Epipe access interface. A fully-specified backbone destination address must be provisioned for each PBB Epipe instance to be used for each incoming frame on the related Epipe L2 access interface. If the backbone destination address is not found in the B-VPLS forwarding database, then packets may be flooded through the B-VPLSs.

To enable an Epipe service with PBB, the Epipe site is configured as a PBB site and functions similarly to a VPLS I-Site. This can only be specified during the site's creation. On the Epipe PBB site, you select a B-Site that acts as the tunnel for the Epipe. You also specify the destination B-MAC address of the remote PE where the other site is located. Figure 71-6 shows a simplified view of this configuration.

Figure 71-6 Epipe service link to a B-VPLS



See the *7750 SR OS Services Guide* for more information about PBB.

BGP Auto Discovery

BGP Auto Discovery enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. This allows each PE's configuration to consist only of the identity of the VPLS instance established on a specific PE, and not the identity of every other PE in that VPLS instance. If you need to change the VPLS topology, only the affected PE's configuration needs to change. Other PEs automatically discover the change using MP-BGP and adapt themselves accordingly. In contrast, if the BGP AD functionality is not used, you must then explicitly configure each PE router with the identities of all the other PEs in a specific VPLS.

You must assign a single, globally unique VPLS-ID to each VPLS (that is, the same value for all sites to the same VPLS across the entire network). The VPLS-ID eliminates the possibility of a collision between VPLSs belonging to different service providers.

There is also a globally unique Route Distinguisher (RD) ID associated with a VPLS. Each site also needs a unique ID that is a BGP NLRI. The PE address does not have to be globally routable, but it must be unique within the VPLS. The PE ID can be the PE router ID, for operational convenience.

Each site must also be associated with one or more RT Extended Communities, and the RTs control the distribution of NLRIs.

Each PE distributes the NLRI for each of its sites, with itself as the BGP next hop, and with the appropriate RT for each NLRI. A PE with a specific RT imports all NLRIs that have that same RT (and learns the other PEs addresses through their next hops). H-VPLS can be configured by using multiple RTs.

In summary, the BGP advertisement for a specific site in a PE includes:

- An NLRI. This is the VSI-ID.
- A BGP next hop equal to the loopback address of the PE.
- An extended community attribute containing the VPLS-ID.
- An extended community attribute containing one or more RTs.

Targeted-LDP [(T-)LDP] signaling is set up for the point-to-point PWs between sites using the selected (T-)LDP sessions corresponding to the remote PE(s) that have been recently added to their list.

To auto-create a Spoke-SDP, a PW Template must be created and pushed down to the NE. The SAM policy distribution mechanism is used to send out the template and maintain consistency in the network. The template selection is at the PE level, not at the service level, because not all PEs are capable of supporting BGP AD and some VPLS sites may not support BGP discovery.

Consider the following with regard to tunnel creation:

- If you plan to use BGP AD for all or part of the VPLS, you must not enable automatic mesh SDP binding creation.
- A provisioned PW to a specific remote PE takes precedence over one that is auto-discovered using BGP AD. In other words, if there is an existing SDP binding available, the router selects this existing binding and does not automatically create a new one.
- When the 5620 SAM auto-tunnel creation function is being used for non-BGP AD VPLSs, the automatically-created components are excluded from discovery. Also, you cannot select an automatically-created SDP or SDP binding when you create a service tunnel that is to be used as part of a BGP AD VPLS.

A 5620 SAM-managed VPLS or H-VPLS may consist of various site types located on different PEs, and which in turn, may be of differing versions. Due to these possibilities, some restrictions apply in terms of using Auto Discovery. For example, an M-VPLS site cannot be in the same service with a regular site. However, BGP AD-enabled sites and regular sites can be components of the same VPLS.

BGP VPLS

BGP VPLS is an extension of the VPLS concept. When configured as a BGP VPLS, such a service can interconnect with another BGP VPLS across different VPLS domains.

The control plane of the BGP VPLS provides auto-discovery and signaling capability. In this context, auto-discovery is a means for a PE router to discover other remote PE routers that are members of a given VPLS. The signaling function enables a PE router to know which pseudowire label a given remote PE router will use when sending the data to the local PE router. The BGP VPLS control plane carries sufficient information to provide the auto-discovery and signaling functions concurrently.

Some of the major features of the Alcatel-Lucent BGP VPLS solution include:

- The data plane is identical with the BGP AD (LDP VPLS) solution. For example, VPLS instances are interconnected via a pseudowire mesh. Split horizon groups may be used for loop avoidance between the pseudowires.
- Addressing is based on a two-byte VE ID assigned to the VPLS instance.
- The target VPLS instance is identified by the Route Target (RT) contained in the MP-BGP advertisement (extended community attribute).
- Auto-discovery is MP-BGP based.
- Pseudowire label signaling is MP-BGP based. As a result, the BGP NLRI content also includes label related information such as block offset, block size, label base, and so forth,

The Alcatel-Lucent BGP VPLS solution is compliant with RFC 4761.

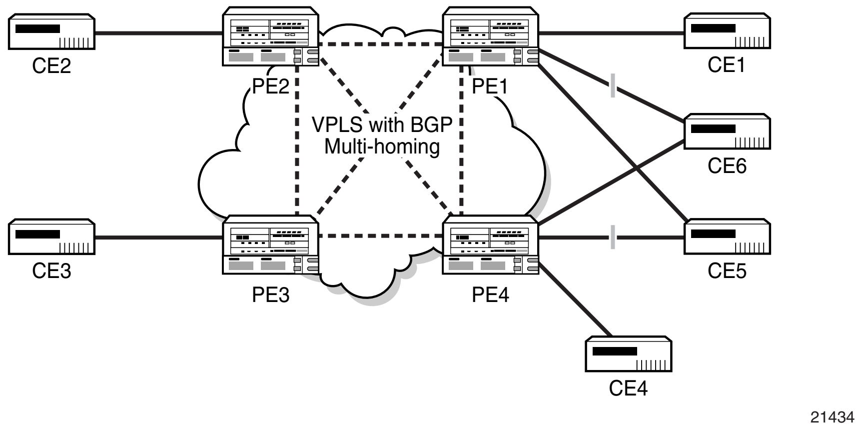
See the *7750 SR OS Services Guide* for more information regarding BGP VPLS.

BGP VPLS Multi-homing

The 5620 SAM allows BGP VPLS multi-homing to be established for CEs and access PEs by first configuring the multi-homing VPLS sites and then assigning the same multi-homing site ID to each.

Figure 71-7 shows an example of this approach, where a VPLS contains certain CEs that are multi-homed to pairs of VPLS PEs.

Figure 71-7 CE Multi-homing in VPLS



The BGP/LDP-signaled PW infrastructure (shown as the cloud at the center) is used to interconnect the VSIs between PEs. In this example, CE5 and CE6 are dual-homed to PE1 and PE4. To avoid loops, only one SAP must be active at any point in time between any multi-homed CE (such as CE5 or CE6) and its pair of connected PEs (such as PE1 and PE4). The others are blocked. Service providers use their MP-BGP on PE1 and PE4 to control the activation of the SAPs connected to the same customer site.

Other CE topologies (for instance, square connectivity) where, for example, CE1 and CE4 are part of the same customer site (and are themselves interconnected) are also supported.

When multi-homing a VPLS site using BGP (potentially into different autonomous systems), the PE routers (for example, PE1 and PE4) that are connected to the same customer site (for example, CE5) are configured with the same multi-homing ID. In this way, a loop-free topology is constructed using a routing mechanism such as BGP path selection. When a BGP speaker receives two equivalent NLRIs, it applies standard path selection criteria such as local preference and AS path length to determine which NLRI to choose.

Two VPLS NLRIs are considered equivalent from a path selection perspective if the following are identical:

- Route distinguisher
- Multi-homing ID

MVR on VPLS

MVR on VPLS is a bandwidth optimization method for applications on a broadband services network. At the port level, MVR allows a VPLS end user to subscribe or unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances without requiring that the stream be part of the customer VPLS.

MVR on VPLS is a mechanism through which the supporting devices are able to participate in a multicast distribution system. Separate, dedicated VLANs must be constructed specifically for multicast traffic distribution.

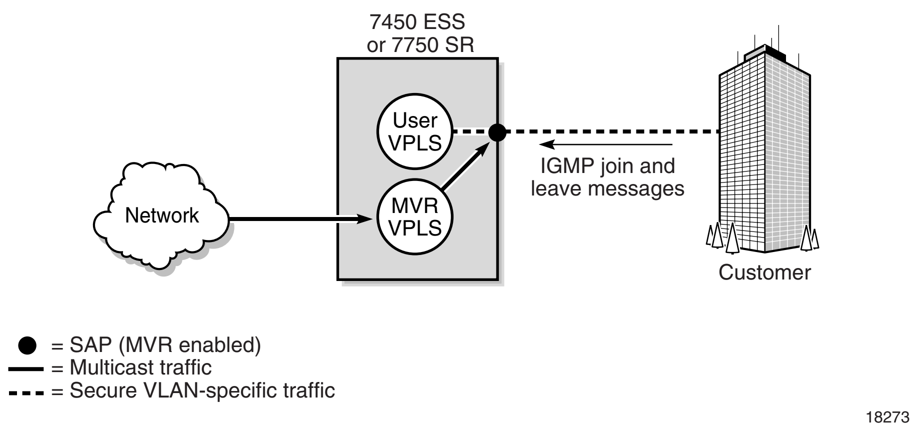
MVR assumes that hosts join and leave multicast streams by sending IGMP join and leave messages. The IGMP join and leave messages are sent inside the VPLS to which the host port is assigned. The multicast VPLS is shared in the network while the hosts remain in separate VLANs. For example, two user VPLS that are bound to the same MVR VPLS cannot exchange any information, but the same multicast service can still be provided to them.

An MVR VPLS is a VPLS that is responsible for sending multicast traffic through the network. An MVR VPLS is associated with a multicast package policy and has MVR-enabled sites. The MVR VPLS is configured to distribute certain multicast streams. An MVR VPLS can also be configured as a user VPLS to receive multicast traffic.

A user VPLS is a VPLS that contains SAPs that can receive multicast traffic from an MVR VPLS. Each SAP must be configured individually to use a specific MVR VPLS. Any VPLS, including an MVR VPLS, can be used as a multicast receiver for an MVR VPLS. IGMP and/or MLD snooping must be enabled on each site.

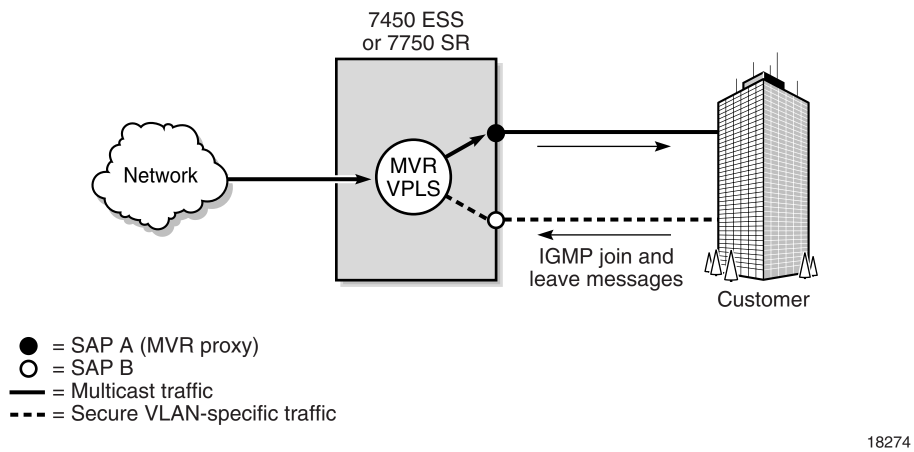
Figure 71-8 shows an example of MVR on VPLS. MVR reacts only to join and leave IGMP messages from the multicast groups configured for the MVR VPLS with which the user VPLS is associated. Join and leave messages from all other multicast groups are managed by IGMP and/or MLD snooping. Therefore, several MVR VPLS instances can be configured, each with its own set of multicast channels.

Figure 71-8 MVR on VPLS



In some situations, such as when a host is connected to a 7301 ASAM, the multicast traffic cannot be sent from the MVR VPLS to the VLAN on which the IGMP message was received (standard MVR behavior) but to another VLAN. This configuration is known as MVR by proxy. The 7450 ESS, 7750 SR, 7710 SR allow multicast traffic to be sent to a SAP other than the SAP from which the IGMP message originated. When configuring MVR by proxy, you must indicate the MVR VPLS on which the multicast channel is available and the SAP to which the multicast traffic must be copied. Figure 71-9 shows an example of MVR by proxy.

Figure 71-9 MVR by proxy



Configuring MVR on VPLS using the 5620 SAM involves the following steps.

1 Configure PIM before configuring MVR. See chapter 31 for more information.

2 Create a multicast package policy for all supporting NEs in an MVR VPLS. See chapter 49 for more information.

 Alternatively, you can configure NEs individually in an MVR VPLS using a routing policy. See Procedure 30-11 for more information.

3 Create the MVR VPLS. See Procedure 71-1 for more information.

- Associate the multicast package policy with the service, which indicates that a VPLS is an MVR VPLS.
- Specify the VPLS sites that are the sources of the multicast groups. MVR must be enabled on each site.
- Configure SAPs only if you are configuring the MVR VPLS to be a user VPLS as well. See Procedure 71-1 for more information about configuring a user VPLS.

4 Create the user VPLS. See Procedure 71-1 for more information.

- The SAPs are standard host access points.
- Configure IGMP and/or MLD snooping and MVR on each site.
- Associate the MVR VPLS with each SAP for which access to multicast traffic is needed. This association means that IGMP requests received at that SAP for a multicast group are fulfilled as long as the multicast group being requested is included in the multicast package policy of the MVR VPLS. After the SAPs in a user VPLS have been associated with a specific MVR VPLS, the SAP becomes known to the MVR VPLS.

5 If using MVR by proxy, configure a VPLS SAP that is to act as the MVR proxy. See Procedure 71-1 for more information.

In a situation in which an MVR VPLS has VPLS sites that do not support MVR, the following conditions apply.

- The ability to configure MVR is not available for the VPLS sites and SAPs of a device that does not support MVR.
- Multicast package policies are not distributed to the devices that do not support MVR.

GSMP group on VPLS

The edge devices determine the circuit that opens an ANCP session. ANCP provides status and control information such as current line rate and port-up and port-down messages to the edge devices. The edge devices perform the following functions:

- adjust the H-QoS subscriber scheduler with the correct rate
- raise an alarm when the rate goes below a set threshold
- send DSL line OAM commands to complete OAM tests

A GSMP group is created under the GSMP tab of the VPLS site form. Multiple groups can be defined and different ANCP capabilities can be associated with different groups. A neighbor can be defined in a GSMP group. Multiple neighbors can be configured for each group.

Note — A GSMP group must be configured on VPLS, MVPLS or VPRN for an ANCP session to open.

L2 management interfaces on VPLS

L2 management interfaces act as a host. L2 management interfaces are created the same way out-of-band interfaces are created on VPLS. L2 management interfaces are used for CPM protocols such as telnet, SSH, SNMP, ping, and ANCP.

CPM filtering is used to limit access to L2 management interfaces.

Routed VPLS

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS service on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. While an IES or VPRN IP interface can only be bound to a single VPLS site, the service context containing the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the routed VPLS binding is dependent upon the operational state of the VPLS site, and whether the IP interface binding is enabled on the VPLS site.

This functionality is limited to supporting devices.

Note 1 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form or from an IES or VPRN access interface form, routed VPLS path.

Note 2 — The routed VPLS binding will not be operationally up until the Enable IP interface binding parameter is set to true and the VPLS site is operationally up. See Procedure 71-1 for more information.

FIBs

The FIB is the set of information that represents the best forwarding information for a destination. A FIB entry is analogous to a static MAC address, and every computer and network node has a MAC address that is hardware-encoded. In 5620 SAM, static MAC addresses can be also created on VPLS endpoint objects, access interfaces, and service circuits.

The edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. Devices perform MAC-address learning to reduce the amount of unknown destination MAC address flooding. The edge devices learn the source MAC addresses of the traffic arriving on their access and network ports. You can also specify and manage static MAC addresses using the FIB entries table.

Each device maintains a FIB for each VPLS instance. Learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating sites using the service. Unknown destination packets (i.e., the destination MAC address has not been learned) are forwarded on all LSPs to the participating devices for that service until the router responds and the MAC address is learned by the device associated with that service.

Note — Each VPLS FIB entry consumes system resources. The devices allow you to set the maximum number of MAC entries allowed in a VPLS instance to prevent a VPLS instance from consuming a disproportionate amount of resources.

The size of the VPLS FIB can be configured with a low watermark and a high watermark expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared.

MAC learning

Like an L2 device, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). In each VPLS, there are independent aging timers for locally learned MAC and remotely learned MAC entries in the FIB. A local MAC address is a MAC address associated with an access interface, because it ingressed on a SAP. A remote MAC address is a MAC address received using a service tunnel from another device that is part of the VPLS.

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

MAC learning can also occur for Split Horizon Groups (SHG) but with accompanying risks. For example, in an L2 environment of an SHG, hosts—among whom mutual communication is disallowed—can launch DoS attacks by sending a flood of packets that source an uplink MAC address to unprotected customer SAPs.

This situation can be managed by controlling MAC learning on the SAPs and SDPs in the following way: when a frame arrives at a protected SAP or SDP, the MAC is applied to its learning table; when a frame arrives at an unprotected customer SAP or SAP containing the address of a protected source MAC address, the frame is immediately dropped and not learned by the unprotected SAP. As a result, the unprotected SAP does not know the MAC address of the uplink and, therefore, cannot use it to flood packets to other SAPs in the SHG. You can create a list of protected MAC addresses and configure the behavior of a SAP that receives a frame that contains a protected source MAC address or an unprotected destination MAC address.

MAC move

A sustained high MAC re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the MAC move feature is an alternative way to protect the network against loops.

When enabled on a VPLS, MAC move monitors the re-learn rate of each MAC. If the rate exceeds the configured allowed limit, it disables the SAP on which the source MAC last arrived. The SAP can be disabled permanently or for a length of time that grows linearly with the number of times the SAP is disabled.

There is also the option of marking a SAP as non-blockable, which means that when the re-learn rate exceeds the limit, another SAP—one that is blockable—is disabled instead. When the MAC move parameter is set to blockable, ports can be blocked in a specific order depending on the number of times the re-learn rate exceeds the configured threshold period.

MAC move is configurable on VPLS SAPs and VPLS spoke SDPs. Blocking information for an object is displayed on the MAC move configuration form for the object. This information includes:

- the number of MAC learning retries that remain before blocking occurs
- the time that remains before the blocked object is unblocked
- the order of blocking, starting with tertiary, secondary and primary

Flooding

Traffic that is normally flooded throughout the VPLS can be rate limited on SAP ingress through the use of Service Ingress QoS Policies. In a Service Ingress QoS Policy, individual queues can be defined per forwarding class to provide shaping of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic. You can also specify how to classify frames.

Multiple services and service types can be configured on a port. VPLS spanning tree protocols are configured on a per-service site basis, not a per-port basis, thus, multiple instances of STP per site are supported. Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service.

The flooding mechanism and the way that the Interior Gateway Protocol (IGP) operates ensure that no packets are duplicated on any interface. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and duplicate packets can traverse the network. The STP is designed to prevent multiple SAPs from forwarding a packet into the VPLS

Spanning tree protocols

The 5620 SAM supports RSTP for VPLS instances and maintains support for legacy STP implementations. STP on the 7750 SR and 7710 SR incorporates an optimized and compatible implementation of IEEE 802.1D which attempts to eliminate STP blocking of links in the core of the VPLS. STP on the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7450 ESS is used to guarantee that service tunnels are not blocked in any circumstance while not imposing artificial restrictions on the placement of the root bridge in the network. To provide this support, all mesh service tunnels are configured as root ports or designated ports.

RSTP, which is the default STP mode managed by the 5620 SAM, is compliant with IEEE standard 802.1D-2004. Other available STP types include an RSTP variant with 802.1w-2001 backward compatibility, an STP variant that is compliant with 802.1w-2001, and MSTP, an STP variant that is compliant with 802.1s-2002. The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7750 SR, and 7710 SR support MSTP.

The 5620 SAM verifies STP parameters that are configured within each VPLS instance. However, it does not check the compatibility of STP configurations between interconnected VPLS instances.

IGMP snooping

IGMP snooping allows a device to snoop packets sent between IP multicast routers or switches and IP multicast hosts to learn the IP multicast group membership. The device checks the IGMP packets for the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is forwarded to all ports, which is the same as broadcast traffic. IGMP snooping ensures that multicast traffic is only forwarded to ports that are members of the specific multicast group, which reduces the amount of multicast traffic passing through the device.

You can enable IGMP snooping for VPLS on Release 1.0 R4 or later of the 7210 SAS-E, Release 1.1 R6 or later of the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP, the 7450 ESS, 7710 SR, and 7750 SR, and Release 6.4.2 R1 or later of the OS 9700E and OS 9800E. You can enable IGMP snooping for VPLS sites, access interfaces, and spoke SDPs on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP. A database of group members per VPLS instance is built by listening to IGMP queries and reports from each SAP and SDP of a service site. The reports are forwarded to the multicast routers.

IGMP snooping is not supported when MAC subnetting is enabled.

MLD snooping

Multicast Listener Discovery snooping is essentially the IPv6 version of IGMP snooping. The guidelines and procedures are very similar to IGMP snooping.

When MLD snooping is not enabled, L2 switches treat multicast traffic like an unknown MAC address or broadcast frame, that is, the frame is flooded out on every port of a VLAN. When MLD snooping is enabled, switches snoop the frame's L3 header for more efficient switching. In the context of IP multicast, only hosts that have expressed interest in receiving packets for the multicast groups have the frames forwarded to them.

The 7x50 and 7710 SR routers allow the enabling of MLD snooping for VPLS. A database of group members (per VPLS instance) is built by listening to MLD queries and reports from each SAP and SDP of the instance. These reports are forwarded to the multicast routers, if any are present.

MLD snooping is not supported when MAC subnetting is enabled.

Consider the following:

- Multicast groups can be learned (using the destination IP addresses of multicast packets) through MLD snooping or by static configuration at the port.
- The Fast leave feature modifies the membership leave mechanism by terminating the session immediately, rather than issuing a group-specific query to check if other members are still present on the network. Therefore, if a port (SAP or SDP) is configured for Fast leave, the session is terminated immediately without checking if the port also has other hosts subscribed to that same multicast group.
- A multicast router retains a list of multicast group memberships for each attached network. Therefore, a multicast router can assume the role of querier or listener. However, there can be only one querier per physical network.
- MLD snooping statistics are collected for each NE port, SAP, or SDP binding, and are viewable from the Statistics tab of a VPLS site properties form.
- The 5620 SAM supports MLDv1 and MLDv2.
- The 5620 SAM supports MVR.
- MLD snooping can co-exist with IGMP snooping and PIM snooping.
- MAC-based forwarding entries can be built using MLD snooping results.

PIM snooping

Protocol Independent Multicast snooping for VPLS allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS. The VPLS PE then forwards multicast traffic based on the multicast states.

When all receivers in a VPLS are IP multicast routers running PIM, multicast forwarding in the VPLS can be efficient when PIM snooping for VPLS is enabled. After PIM snooping is turned up at the service level, all sites have PIM snooping configured and are set to the down state, by default. If any site does not support this feature, the 5620 SAM treats it as having PIM snooping turned off.

Since PIM snooping operates on PIM Hello packets as well as Join/Prune packets, PIM neighbors of the current router are learned by snooping on Hello packets. Therefore, in a meshed VPLS, every node learns from every other node's Hello packet and considers that node as a neighbor.

VPLS PE routers only snoop on PIM Hello and Join/Prune packets; they do not generate PIM messages on their own. Therefore, when PIM snooping is configured at the service level, all CE routers must have Join/Prune suppression disabled. If a VPLS PE router detects a condition where Join/Prune suppression is not disabled on one or more CE routers, the PE router puts PIM snooping into a non-operational state for the entire service. A trap on the PE is generated to report this condition and an alarm is raised to the 5620 SAM operator. To bring PIM snooping back to the operational state, PIM snooping must be disabled and then re-enabled.

Since PIM uses state refreshes, VPLS PE routers may not learn multicast states from all the CE routers, if PIM snooping was just enabled or the all snooping state was just cleared, until the next refresh.

To avoid traffic interruption, PIM snooping should hold up its operations for a period of time (60 seconds, if default timer is used). During this period of time, multicast traffic is flooded in the VPLS just like snooping was not enabled. SAM should have this hold-up timer configurable on VPLS properties panel having range 0-120 with 60 secs as default.

A variety of statistics are gathered for PIM snooping operation and are available for viewing and analysis in the PIM Snooping tab of a VPLS configuration form.

PIM snooping is not supported when MAC subnetting is enabled.

PIM snooping only supports IPv4.

Split horizon groups

SHGs control traffic that flows through SAPs or spoke SDPs for a VPLS site. SHGs prevent a packet received on a SAP within the group from being propagated to other members of the group.

SHGs are defined when you create or modify a VPLS site. You can create multiple SHGs for a VPLS site. SHGs can support a mix of spoke SDPs and SAPs. When you create SAPs or spoke SDPs they can be associated with an SHG.

Users can:

- configure, modify, or delete SHGs on a VPLS site
- associate SAPs or spoke SDPs with SHGs

Residential split horizon groups

RSHGs are SHGs with the Residential parameter enabled. SAPs that are associated with RSHGs are called lightweight SAPs. RSHGs use dual-pass queue optimization and do not support downstream broadcast or multicast traffic.

Users can:

- configure, modify, or delete RSHGs on a VPLS site
- associate SAPs or spoke SDPs with RSHGs

Note — If a SAP or spoke SDP is associated with an RSHG, then the following apply:

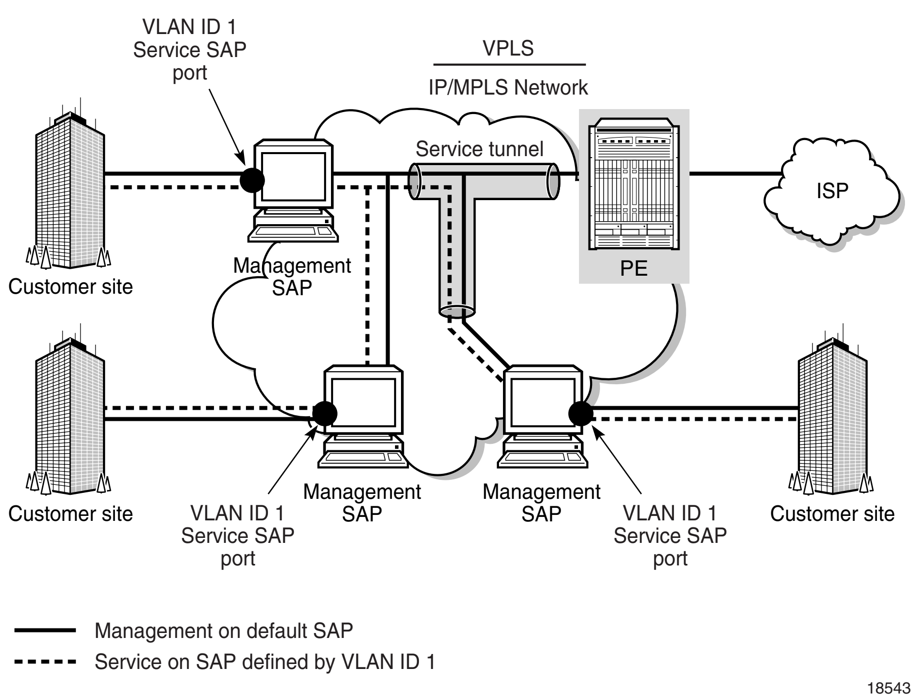
- MAC pinning is enabled by default and cannot be disabled for the interface
- IGMP snooping, MLD snooping, and MVR are not configurable for the interface

Default SAPs

The 5620 SAM allows you to create a default SAP that you can use in an L2-based service to perform management tasks or to deliver a specific class of end-user service. One default SAP can be defined on any dot1q encapsulated Ethernet port. You can create a default SAP by specifying an outer encapsulation value of 4095 or *. If OSSI is used, the outer encapsulation value is always 4095.

Figure 71-10 shows a default SAP used as a dedicated management port.

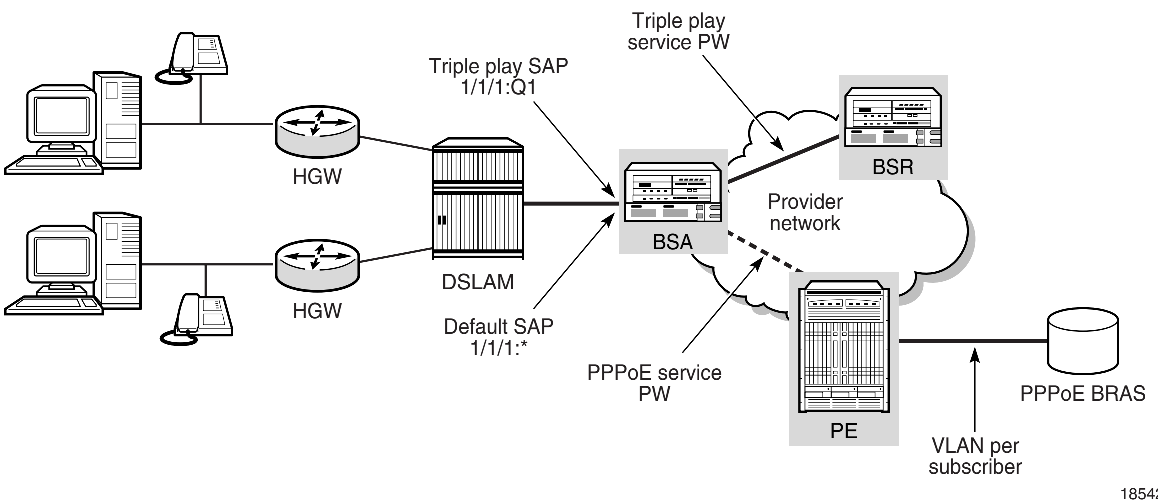
Figure 71-10 Default SAP as a dedicated management port



The dotted line shows that a business customer uses an entire port to access an L2 service using a VLAN tag ID 1, which is transparent to the network service provider. The service provider has assigned a default SAP for management of the customer network, as shown by the solid line. The customer uses one SAP for service delivery, and the service provider uses the default SAP to manage the customer network.

Default SAPs can also be used to differentiate one class of service from another on a single port. In Figure 71-11 the service provider can deliver aggregated high-speed Internet services on a single default SAP for multiple hosts while applying tags that assign one VLAN per host. At the same time, each of the remaining SAPs on the same port can be deployed for higher-level services, such as triple play delivery, in which multiple or individual hosts are assigned to a single SAP. Using such differentiated SAPs is efficient and significantly increases network scalability, because of the reduced number of SAPs allocated to various customers.

Figure 71-11 Default SAP to differentiate subscriber services



Layer 2 protocol tunneling termination

L2PT allows service providers to preserve the VLAN and Layer 2 protocol configurations of individual customers without impacting the traffic of other customers across the core network. L2PT termination allows Layer 2 PDUs to be transparently tunneled across the core network, avoiding interaction between the network provider and customer protocols.

Transparent L2PT is performed on the ingress side of every SAP or spoke SDP of the PE routers configured with L2PT termination. L2PT tunnels PDUs by overwriting the customer PDU of the destination MAC address in an Ethernet packet the multicast MAC address 01-00-0c-cd-cd-d0. The Ethernet packet is then transparently tunneled over the core network to a peer PE router. The peer PE router at the egress side of the tunnel restores the MAC address and the L2 protocol so that packets are forwarded to all ports in the same VLAN.

L2PT termination can only be enabled if STP is disabled on the VPLS.

BPDU translation

VPLS networks typically interconnect customer sites that use different access technologies, such as Ethernet and bridge-encapsulated ATM PVCs. Because of this, BPDU translation may be necessary to provide end-to-end interconnectivity.

If BPDU translation is enabled on a SAP or spoke SDP, the device intercepts all BPDUs and performs the required translation.

BPDU translation can be enabled only on a SAP or spoke SDP binding if STP is disabled on the VPLS.

DoS protection

To protect a VPLS from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPLS L2 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPLS L2 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPLS L2 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 21-3 for information about creating a DoS protection policy.

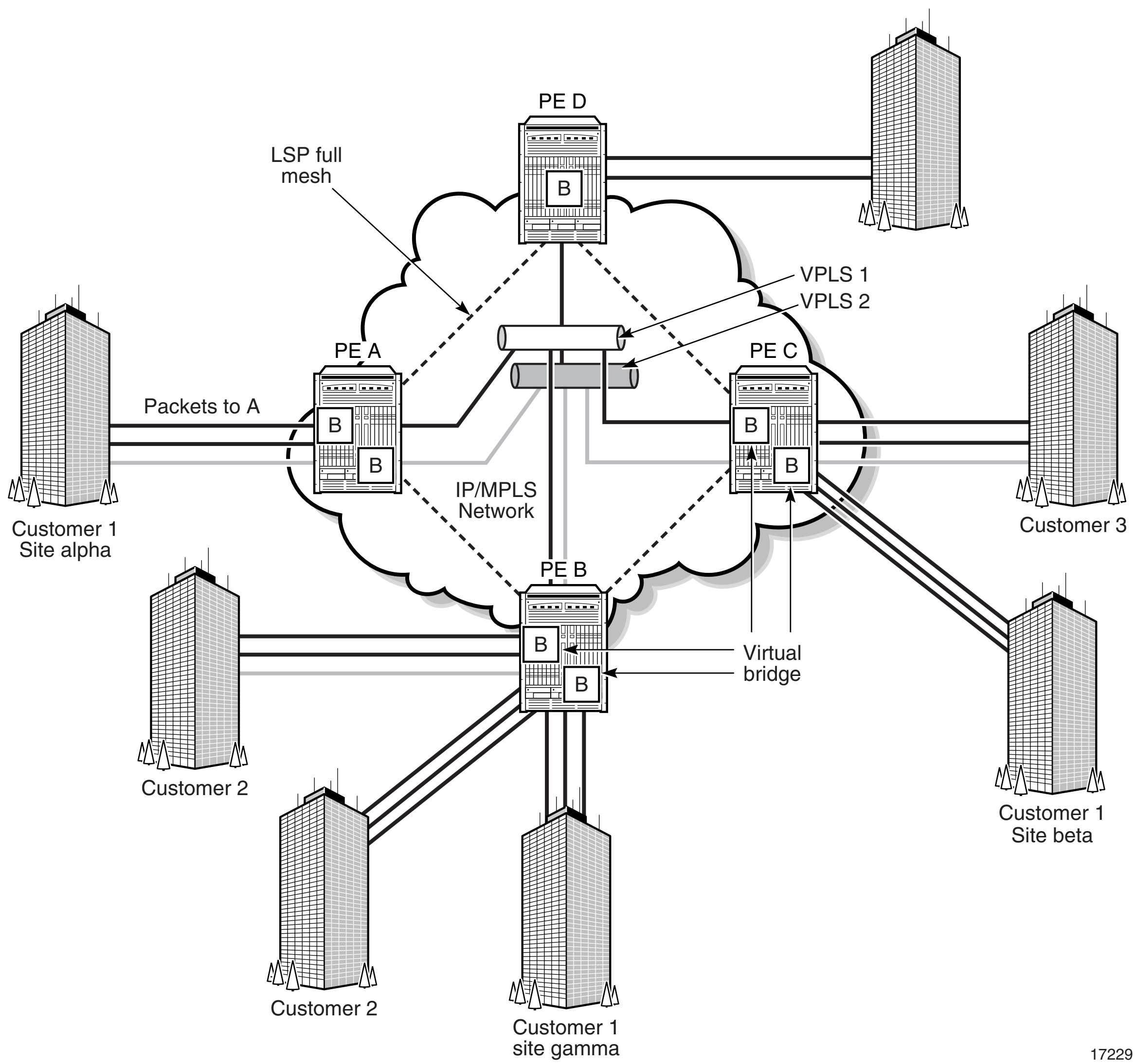
Copying and moving SAPs between ports

You can copy and move SAPs between ports. See “Moving and copying SAPs between ports” in chapter 20 for more information.

71.2 Sample VPLS configuration

Figure 71-12 shows a sample VPLS configuration.

Figure 71-12 Sample VPLS



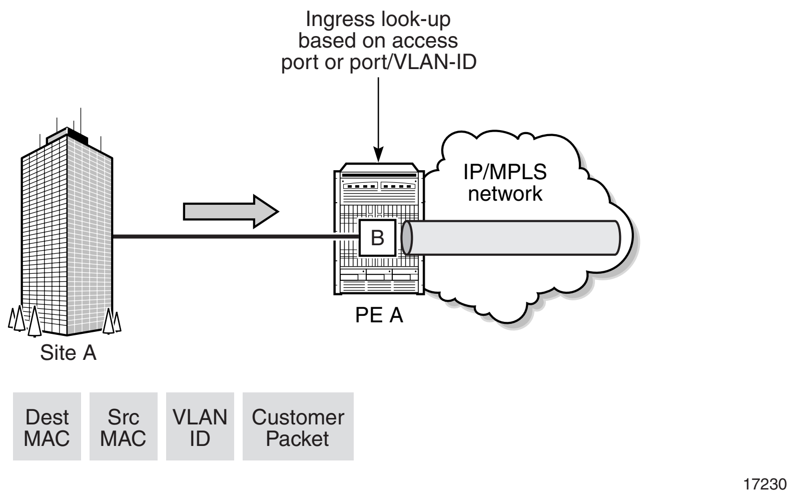
VPLS 1 is a distributed service, which consists of customer 1 connected to PE A, PE B, and PE C, at sites alpha, gamma, and beta, respectively. All three customer sites belong to VPLS 1.

In the following example, Customer 1 wants to send data from site alpha to site beta.

Customer 1 packets arriving at PE A are associated to the appropriate VPLS 1 for that customer, based on the combination of the access port and the dot1q (VLAN ID) in the packet. PE A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the access port on which it was received.

PE A is sending the packets to PE C. The destination MAC address in the packet is looked up in the FIB table of PE A for the VPLS instance, as shown in Figure 71-13.

Figure 71-13 Packet forwarding by ingress router PE A



The destination MAC address in the FIB table has one of two values:

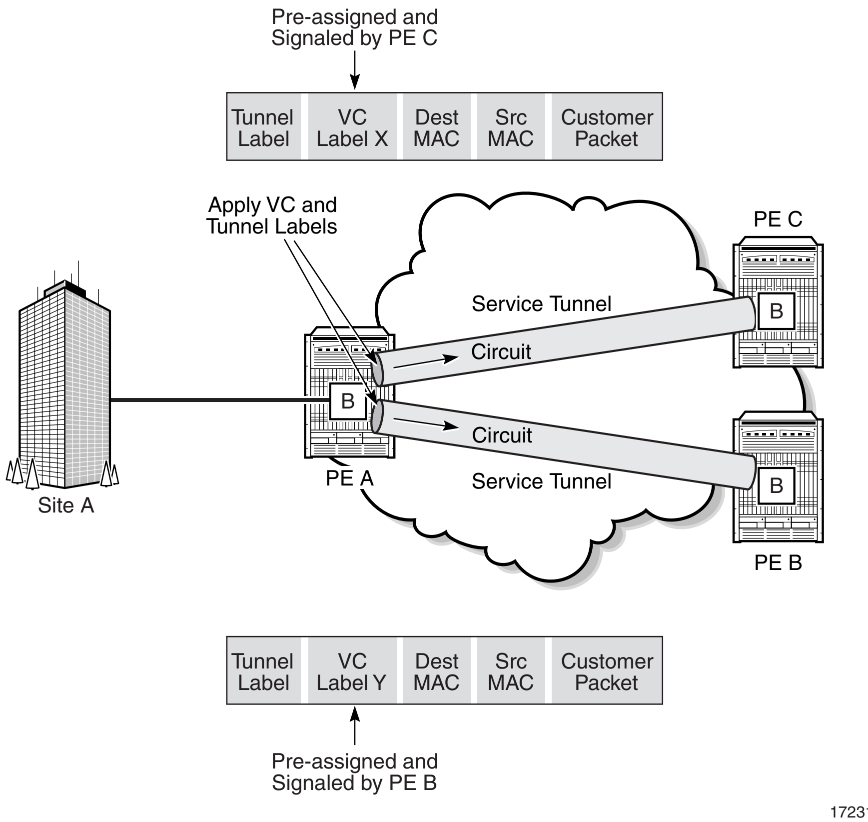
- known
- unknown

If the destination MAC address is known by PE A, an existing entry in the FIB table identifies the far-end PE C and the service VC label (VLAN ID) used to send the packets from PE A to PE C. PE A chooses a transport LSP to send the packets to PE C. The packets from the customer 1 site alpha to site beta are sent on the LSP after the VC label is removed and the transport label is added to the packet, as shown in Figure 71-13.

If the destination MAC address is not known by PE A, PE A floods packets to both PE B and PE C, which are both part of VPLS 1. PE A uses the VC labels (VLAN IDs) that PE B and PE C previously signaled for this VPLS 1.

As shown in Figure 71-14, the packets from PE A are transported across the core IP/MPLS network.

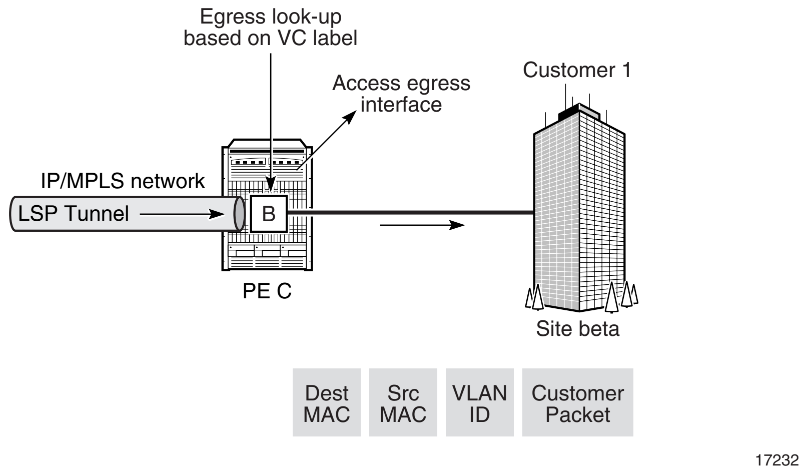
Figure 71-14 Packet forwarding from PE A across the core IP/MPLS network



The core routers are LSRs that switch the packets towards their destination based on the tunnel label, also called a transport label. The core routers are not aware that the packets belong to a VPLS.

When the packets from PE A arrive at PE C, PE C removes the tunnel label to reveal the VC label that associates the packets with VPLS 1, as shown in Figure 71-15.

Figure 71-15 Packet forwarding by egress router PE C



PE C learns the source MAC address of PE A and creates an entry in its FIB table that associates the MAC address and the VC label with PE A. The destination MAC address is looked up in the FIB table. It has one of two values:

- known
- unknown

If the destination MAC address is known by PE C, an existing entry in the FIB table identifies the local access (egress SAP) port used by VPLS 1 site beta and the service VC label (VLAN ID) that needs to be added to send the packets from PE C to customer 1.

If the destination MAC address is not known by PE C, PE C floods packets to all local access ports that belong to VPLS 1.

Assuming the core IP/MPLS network has already been configured, the following high-level tasks are required to configure this sample VPLS.

Table 71-1 Sample VPLS configuration

Task	Description
1. Configure policies as required	Policies must be configured before service creation. The following key policies can be applied to resources that are part of a VPLS: • Access ingress and access egress policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open the access ingress and egress interface policy forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL MAC filter policies. These policies specify access control lists based on MAC addresses. You can specify MAC learning for access ports or tunnels. Choose Policies→Filter→ACL MAC Filter to open the ACL filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form. • DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form.
2. Configure ports as access ports for use in the service	Choose a port from the navigation tree, right click on the port, and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels, as required.	Service tunnels, or SDPs, are automatically created if there are no tunnels between the source and destination devices. You must choose GRE or LDP as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Service tunnels carry service traffic between edge-managed routers. Services are associated with service tunnels by SDP bindings during service configuration. During service creation, you can also configure the 5620 SAM to automatically create SDP bindings to associate service tunnels with a service. In this case, you do not have to create service tunnels before you create the service.
4. Create and configure Customer 1.	Choose Manage→Service→Customers to open the customer manager form and create the customer.

(1 of 3)

<table>
<tr><th>Task</th><th>Description</th></tr>
<tr><td>5. Create and configure VPLS 1.</td><td>
Specify Customer 1 as the customer for the VPLS.
Configure MVR for the VPLS, if required.
Configure a GSMP Group and a GSMP group neighbor for the VPLS, if required.
Configure L2 management interfaces, if required.
Specify PE A, PE B, and PE C as the sites for the VPLS.
Specify VPLS STP parameters, if required.
Specify VPLS FIB parameters, if required.
Specify VPLS MAC move parameters, if required.
Specify VPLS MAC flush parameters, if required.
Enable VPLS PIM snooping, if required.
Specify VPLS IGMP snooping parameters, if required.
Specify VPLS MLD snooping parameters, if required.
Create an SHG for the VPLS, if required.
Configure and specify access interfaces on the PE A and PE C sites as the access interfaces for the VPLS to site alpha and site beta. You do the following when you configure interfaces:
Specify the ports for the access interfaces and configure the access interfaces. Ports must be configured as access ports.
Specify the EMG to which the L2 access interface belongs.
Assign ingress and egress QoS policies as required.
Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
Assign ACL filter policies as required.
Assign an accounting policy, if required.
Specify a ToD suite, if required.
Configure STP and FIB forwarding control.
Configure subscriber management parameters, if required.
Assign a DoS protection policy, if required.
Configure VPLS PIM snooping, if required.
Configure IGMP snooping for the interface, if required.
Configure MLD snooping for the interface, if required.
Configure DHCP for the interface, if required.
Configure ARP host configuration, if required.
Configure MVR for the interface, if required.
Configure anti-spoofing for the interface, if required.
Associate MEPs with SDP spoke bindings or SAPs, if required.
Associate virtual MEPs with services, if required.
Configure ANCP, if required.
Configure ATM functionality, if required.

Create and configure service tunnels in both directions.
If the VPLS is a distributed VPLS, configure mesh SDP bindings to connect the VPLS sites. You can also configure the 5620 SAM to automatically create SDP bindings.
</td></tr>
<tr><td>6. Create, update, or configure additional sites or L2 access interfaces for the VPLS.</td><td>
Repeat the above steps as required.
Create an MSAP policy, if required. See Procedure 68-5 for more information about creating an MSAP policy.
Configure the SAP Sub Type to be created. If your SAP is to support a shared SAP model, configure a Regular SAP; that is choose Regular as the SAP Sub Type. If you need to use an MSAP to support the one subscriber per SAP model, choose Capture as the SAP Sub Type and then configure the Capture L2 Interface parameters, which control the DHCP, PPPoE, or ARP triggered creation of MSAPs. See Managed SAP (MSAP) in section 68.1 for more information about creating a Capture SAP and MSAP.
</td></tr>
<tr><td>7. For an HVPLS, use spoke SDP bindings to connect VPLS sites to other sites in the same VPLS, to sites in a different VPLS, or to VLL service sites.</td><td>An HVPLS consists of VPLS sites connected to other VPLS sites in the same or different VPLS, or to VLLs, using spoke SDP bindings. You perform the following when you configure an HVPLS.
Create one or more VPLS and VLL services, as required. See chapter 70 for information about creating a VLL service. See Procedure 71-1 in this chapter for information about creating a VPLS.
Create spoke SDP bindings between the service sites, one in each direction. Specify existing service tunnels and a VC ID for the spoke SDP bindings, as required.
</td></tr>
</table>

(2 of 3)

Task	Description
8. Create a single MVPLS.	Create an MVPLS to run RSTP and to protect redundant spoke SDPs or SAPs in the associated VPLS.
9. Create a composite MVPLS to manage traffic blocking for multiple VPLS.	An MVPLS composite service manages traffic for multiple VPLS with redundant spoke SDPs or SAPs. You perform the following when you configure an MVPLS composite service: • Create a composite service and add the individual MVPLS. • Create spoke SDP connectors between the MVPLS.

(3 of 3)

71.3 Workflow to create a VPLS

The following workflow lists the high-level steps required to create a VPLS. As a prerequisite for creating a VPLS, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1.
- the access ports for the service are created; see chapter 20 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.

1 Create and configure a VPLS. See Procedure 71-1 for all devices that suppport the creation of a VPLS except for 7210 SAS devices. See Procedure 71-2 for 7210 SAS devices.

i Define the service type as VPLS.

ii Ensure the LSP network is configured when the transport mechanism is MPLS.

iii Configure HVPLS spoke redundancy, if required.

iv Specify the sites for the service.

v Create endpoints for redundant configuration, if required.

vi Create a spoke SDP binding under any endpoints you created, if required.

vii Configure the split horizon group parameters, if required.

viii Configure DHCP, if required.

ix Configure MVR, if required.

x Configure GSMP group and GSMP group neighbor parameters, if required.

xi Specify the STP parameters, if required.

xii Create MSTP instances and associate VLANs, if required.

xiii Specify protected MAC addresses, if required.

2 Create L2 access interfaces for the VPLS sites, as required. See Procedure 71-3.

i Specify aggregation on a service basis, or across a card or port.

ii Configure MSAP policies, if required. Create an MSAP Policy to control how the parameters are applied to an MSAP when it is automatically created. See Procedure 68-5 for more information.

iii Configure the SAP Sub Type as Regular or Capture, as required. Regular is the default value used for the creation of a SAP and Capture is the value used to enable the automatic creation of an MSAP. That is, you create a Capture SAP to enable the creation of an MSAP. See Procedure 68-20 for more information about creating a Capture SAP.

iv Assign QoS, scheduling, accounting, ANCP and filter policies.

v Specify MAC ACL filters, if required.

vi Assign a time of day suite, if required.

vii Configure the FIB and STP parameters.

viii Configure subscriber management, if required.

ix Assign a DoS protection policy, if required.

x Configure PIM snooping parameters, if required.

xi Configure IGMP snooping parameters, if required.

xii Configure MLD snooping parameters, if required.

xiii Configure DHCP relay parameters, if required.

xiv Configure ARP hosts, if required.

xv Configure MVR, if required.

xvi Configure anti-spoofing parameters, if required.

xvii Configure queue override parameters, if required.

xviii Configure MEP parameters, if required.

xix Configure ANCP, if required.

xx Configure L2 management interfaces, if required.

3 Create a mesh SDP binding for the VPLS site, if required. See Procedure 71-4.

4 Create a spoke SDP binding for the VPLS site, if required. See Procedure 71-5.

5 Create and enable a video interface for the VPLS, if required. See Procedure 36-3.

6 Configure a site for BGP AD or BGP VPLS, as required. See Procedure 71-6.

7 Configure a site for BGP VPLS Multi-homing, as required. See Procedure 71-7.

8 Perform one or more of the following.

- **a** Re-evaluate the PW Templates associated with a BGP AD or BGP VPLS site, as required. See Procedure 71-8.
- **b** Create an HVPLS. See Procedure 71-9.
- **c** Create an MVPLS. See Procedure 71-10.
- **d** Create a B-site for VPLS or MVPLS. See Procedure 71-11.
- **e** Create an I-VPLS. See Procedure 71-12.
- **f** To create a VPLS or MVPLS B-L2 access interface. See Procedure 71-13.
- **g** Create a VPLS I-L2 access interface. See Procedure 71-14.
- **h** Configure a GNE site on a VPLS service. See Procedure 71-15.
- **i** Force a switchover to a redundant spoke SDP binding. See Procedure 71-16.
- **j** Run an OAM validation test for a VPLS. See Procedure 71-17.

9 As required, modify the FIB entries associated with a VPLS:

- **a** Add or modify FIB entries; see Procedure 71-18.
- **b** To list FIB entries; see Procedure 71-19.

10 As required, view VPLS information:

- **a** View the service topology map associated with a VPLS. See Procedure 71-20.
- **b** View the VPLS operational status. See Procedure 71-21.
- **c** View IGMP snooping queriers. See Procedure 71-22.
- **d** View MLD snooping queriers. See Procedure 71-23.

11 As required, modify a VPLS:

- **a** Using the Manage Services form. See Procedure 71-24.
- **b** Using the topology view. See Procedure 71-25.

12 As required, delete a VPLS. See Procedure 71-26.

71.4 VPLS management procedures

Use the following procedures to perform VPLS creation and management tasks.

Procedure 71-1 To create a VPLS

This procedure applies to all devices that suppport the creation of a VPLS except for 7210 SAS devices. See Procedure 71-2 for 7210 SAS devices.

Note 1 — For OS devices, only the OS 9700E and OS 9800E NEs support the creation of a VPLS.

Note 2 — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for VPLS configuration at the site level:

- General
- Components
- Scripts
- L2 Access Interface
- Forwarding Control
- Mesh SDP Bindings
- Templates
- Faults

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Choose a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes, and the VPLS Service (Create) form displays the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Default Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation
- Profile Name
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Depending on the type of device being configured, the MVR tab is configurable. Assign a multicast package policy to the VPLS, if required.

i Click on the MVR tab button.

ii Click on the Select button to choose a multicast package policy. The Select Multicast Package Policy - VPLS Service - Subscriber form opens.

iii Choose a multicast package policy and click on the OK button. The Select Multicast Package Policy - VPLS Service - Subscriber form closes, and the VPLS Service (Create) form refreshes with the multicast package policy name.

After the multicast package policy is applied to the VPLS, the policy is distributed as the routing policy to all MVR-capable VPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

6 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

7 If you are configuring the service for BGP Auto-Discovery, go to step 8. Otherwise, go to step 11.

8 Click on the BGP AD tab button.

9 Set the BGP AD Administrative Status parameter to Up. The BGP AD Service Identification group appears.

10 Configure the VPLS ID parameter. This parameter must be a unique network-wide ID.

11 Perform one of the following:

a Create a site for the VPLS. Go to step 12.

b Complete service creation if sites, L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 41.

For information on adding a GNE site to a VPLS service, see Procedure 71-15.

12 On the navigation tree, right-click on Sites and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens with a list of available sites.

Note — The options to create either a B-Site or an I-Site are used when you are creating a VPLS that utilizes Provider Backbone Bridging. See "Provider Backbone Bridging in VPLS" in section 71.1 for more information.

13 Select a site and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Description
- MTU
- MTU Check
- Default Mesh VC ID
- Administrative State
- Monitor Access Interface Operational State
- GSMP Administrative State
- PIM Snooping Enabled
- Per Service Hashing for LAG Enabled
- Enable IP Interface Binding
- SAP Type
- Customer VID
- PPPoE Circuit ID
- Tunnel Fault Notification

Note 1 — The Enable IP Interface Binding parameter is configurable only on a 7450 ESS in mixed mode, or a Release 8.0 R5 or later 7750 SR.

Note 2 — The parameters that appear on the VPLS Site (Create) form depend on the device type and release that you are configuring.

Note 3 — Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

Note 4 — If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the facility tunnel MEP.

If you are configuring a 7250 SAS-ES or 7250 SAS-ESA site, configure the following additional parameters:

- Default VC ID
- Inherit Service ID Value
- Enable Secure SAPs
- VPLS Tag
- VC Type

Caution — On the 7250 SAS, Release 2.0, the SAPs and SDPs on a VPLS site will go down when the 5620 SAM is used to configure the site attributes. You must manually reconfigure these SAPs and SDPs back up after configuring the VPLS site.

Note — 7250 SAS-ES NEs must be included in a VPLS ring group before VPLS services can be created or discovered.

15 If you are configuring a 7250 SAS-ES or 7250 SAS-ESA site, go to step 30.

16 Configure MFIB, STP, FIB, and MAC learning protection parameters for the VPLS site, if required.

i Click on the Forwarding Control tab button. The MFIB tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the VPLS site, if required. Otherwise, go to step iv.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

Note 1 — Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay - 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 2 — If you are configuring an MVPLS site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 71-10 for more information about creating an MVPLS.

Note 3 — MSTP is configurable only on the 7450 ESS and 7750 SR.

iv Click on the FIB tab button to configure FIB parameters for the VPLS site, if required. Otherwise, go to step 17.

v Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on fail
- Propagate MAC Flush
- MAC Subnet Length

vi Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number Of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

vii Click on the MAC Protection tab to configure the list of protected MAC addresses.

viii Click on the Create button. The MAC Protection (Create) form opens.

ix Configure the Protected Mac Address parameter.

x Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

xi If you are configuring an MVPLS site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 17.

Note — MSTP is configurable only on the 7450 ESS and 7750 SR.

xii Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

xiii Click on the MST Instances tab button.

xiv Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

xv Configure the parameters:

- Instance Index
- Priority

xvi Click on the VLAN Ranges tab button. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

xvii Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xviii Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xix Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xx Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xxi Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

17 Configure SHCV for the site, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

18 Configure a default gateway for the site, if required.

i Click on the Default Gateway tab button.

ii Configure the parameters:

- Default Gateway IP Address
- Default Gateway MAC Address

19 Configure ingress multicast forwarding, if required.

Note — An Operational Channels tab appears when you access the VPLS Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 46 for information about listing the operational channel parameters.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy form opens.

iii Choose a policy in the list and click on the OK button. The Select Ingress Info Policy form closes and the policy identifier is displayed on the Site (Create) form.

20 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust Count
- Report source address
- Use query source address

21 Create an endpoint for redundancy (dual homing) on the site, if required.

Note — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 45 for more information.

i Click on the Endpoints tab button.

ii Click on the Create button. The VPLS Endpoint (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Revert Time (seconds)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning
- Maximum FIB Entries
- Block On Mesh Failure
- Endpoint Type

If you set the Endpoint Type parameter to Multi Chassis, go to step iv. Otherwise, go to step ix.

iv Configure the EndPoint ID parameter.

v Click on the Select button beside the Peer Name parameter. The Select Multi Chassis Endpoint Peer - VPLS Endpoint form opens.

vi Configure the filter and click on the Search button. A list of multichassis endpoint peers appears.

vii Select a multichassis endpoint peer and click on the OK button to close the Select Multi Chassis Endpoint Peer - VPLS Endpoint form. A dialog box prompts you to click on the OK or Apply button to commit the changes.

viii Click on the OK button.

ix Click on the OK button. A dialog box appears indicating changes are not committed until you click on the OK or Apply button.

x Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears with the new endpoint displayed in the list.

22 If you are configuring an MVPLS site, go to step 24.

23 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Residential
- Restrict Protected Source
- Restrict Unprotected Destination
- Restrict Protected Source Action

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

24 Depending on the type of device you are configuring, the MVR tab is configurable. Configure MVR for the site, if required.

i Click on the MVR tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State
  The Administrative State parameter specifies whether a site is an MVR VPLS site.
- Description
- Use Component Package Policy
- Routing Policy Name

After the multicast package policy is applied to the MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

iii If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

- Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.
- Manually enter a multicast package policy name as the Routing Policy Name parameter value.

iv Click on the User MVR SAPs tab button to view the VPLS SAPs that use the MVR VPLS site, if required.

- Click on the Search button to list the VPLS SAPs.

25 Configure a GSMP group on the site, if required.

i Click on the GSMP tab button.

ii Click on the Create button. The GSMP Group (Create) form opens.

iii Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- OAM Administrative State
- Dynamic Topology Discovery

iv Click on the GSMP Group Neighbor tab button.

v Click on the Create button. The GSMP (Create) form opens.

vi Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

vii Click on OK button. The GSMP (Create) form closes.

26 Configure L2 management interfaces, if required.

i Click on the L2 Management Interfaces tab button.

ii Click on the Create button. The VPLS L2 Management Interface Subscriber (Create) form opens.

iii Click on the General tab to configure the following parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- ARP Timeout (seconds)
- I/F MAC Address

iv Click on the Addresses tab button.

v Click on the Create button. The IP Address (Create) Form opens.

vi Configure the following parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format

vii Click on the OK button. The IP Address (Create) form closes.

27 Configure MLD snooping for the site, if required.

i Click on the MLD Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust Count
- Report source address
- Query source address

28 Depending on the type of device that you are configuring, the MVR (MLD) tab is configurable. Use the MVR (MLD) tab to use MLD snooping on the site. Configure MVR for MLD on the site, if required.

i Click on the MVR (MLD) tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State
  The Administrative State parameter specifies whether the site is an MVR VPLS site.
- Description
- Use Component Package Policy
- Routing Policy Name

The Routing Policy Name parameter is configurable when the Use Component Package Policy is disabled.

After a multicast package policy is applied to an MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site and the previously distributed policy remains on the site.

iii If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

- Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.
- Manually enter a multicast package policy name as the Routing Policy Name parameter value.

iv Click on the User MVR SAPs tab button to view the VPLS SAPs that use the MVR VPLS site, if required.

- Click on the Search button to list the VPLS SAPs.

29 Configure IGMP host tracking, if required.

i Click on the IGMP Host Tracking tab button.

ii Configure the parameters:

- Expiry Time
- Administrative State

30 To create an access interface for the site, perform steps 5 to 54 of Procedure 71-3.

31 To create a mesh SDP binding for the site, perform steps 5 to 25 of Procedure 71-4.

Note 1 — The maximum number of SDP bindings (combined total of mesh and spoke bindings) per service site on an SR NE is 100.

Note 2 — In 5620 SAM release 9.0 R5, the maximum number of sites that can be automatically meshed (mesh SDP bindings) on a VPLS is 100. The previous limit was 50. Automatic creation of a full mesh on a VPLS can be performed in one pass or in several steps, depending on your requirements.

Alcatel-Lucent recommends that users perform the automatic meshing on only 50 sites at a time, since auto-meshing 100 sites may incur a substantial delay in building the network.

Note 3 — You cannot create a mesh SDP binding on a 7450 ESS, 7250 SAS-ES or 7250 SAS-ESA site.

32 To create a redundant spoke SDP binding under an endpoint, perform steps 4 to 43 of Procedure 71-5.

33 To create a spoke SDP binding for the site, perform steps 8 to 43 of Procedure 71-5.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

34 To add a Video interface for the site, perform steps 4 to 12 of Procedure 36-3.

35 Click on the OK button. The VPLS Site (Create) form closes, and a dialog box appears.

36 Click on the OK button. The VPLS Site (Create) form displays the new site on the navigation tree under the Sites icon.

37 To configure the site for BGP Auto-Discovery, BGP VPLS or as part of a BGP VPLS Multi-homing configuration, you must first complete the creation of the site and then perform either Procedure 71-6 or Procedure 71-7, as applicable.

Note — You can see a list of all current BGP VPLS Multi-homing sites in a VPLS multi-homing service on the BGP Multi-homing Sites tab.

38 Repeat steps 12 to 36 to create an additional site for the VPLS, as required.

39 Add protected MAC addresses at the service level, if required. Protected MAC addresses that you add on the site level, as performed in step 16, are automatically added to the service-level MAC protection list.

i Click on the Forwarding Control tab button.

ii Click on the MAC Protection tab button.

iii Click on the Create button. The MAC Protection (Create) form opens.

iv Configure the Protected Mac Address parameter.

v Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS (Create) form.

40 To reserve tunnel bandwidths, click on the Bandwidth tab.

Note 1 — The ability to reserve tunnel bandwidth is only applicable to B-sites on a VPLS configured as a PBB tunnel (that is, as a B-VPLS).

Note 2 — The Bandwidth tab is only available if service CAC is configured; see chapter 6 for information about enabling and disabling service CAC.

i Click on the Bandwidth Reserved Tunnel sub-tab button.

ii For each CoS, enter a value for the CoS Reserved Bandwidth (Mbps) to specify how much bandwidth this tunnel will reserve in the network.

iii Click on the Reserve Bandwidth button. This action checks to ensure that all the active links in the B-VPLS have enough bandwidth to admit the tunnel into the network and book the bandwidth. The tunnel status will be updated appropriately, based on the outcome of the action. Once the bandwidth is reserved, the BW Utilization tab on the applicable Physical Link properties form will also show this tunnel and the bandwidth information (refer to Procedure 5-37).

Note 1 — The reserved bandwidth of the tunnel can be changed at anytime after the service creation. However, if a change to the reserved bandwidth causes the used bandwidth to be greater than the requested change, or if there is insufficient bandwidth in the network to facilitate this change, then it will be denied and an appropriate message is displayed.

Note 2 — Once bandwidth is reserved on the tunnel, any changes to the topology of the B-VPLS (for example, uplinks added, STP state changes, and so forth) will be updated automatically with the correct bandwidth information on the underlying physical links. If there is insufficient bandwidth available when the changes happen, the bandwidth will still be booked on the physical links and the appropriate alarms will be raised.

Note 3 — To unreserve bandwidth of the tunnel after the service creation, you can set all of the configured Cos Reserved Bandwidth parameters back to 0. However, this can only be done when there are no longer any i-services riding on this PBB Tunnel.

Note 4 — After the service has been created, the Tunnel Usage sub-tab shows all the i-services currently using this tunnel and the specific bandwidth usage per service.

41 Click on the OK button. The VPLS Service (Create) form closes.

Procedure 71-2 To create a VPLS on a 7210 SAS device

This procedure applies to 7210 SAS-E and 7210 SAS-D devices.

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Choose a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes and the VPLS Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Default Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation
- Profile Name
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled and the Profile Name parameter is left blank.
- GSMP Administrative State
- PIM Snooping Enabled
- OLC State
  This parameter is configurable when you click on the Apply button.

5 On the navigation tree, right-click on the Sites icon and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens with a list of available NEs.

6 Choose a 7210 SAS-E and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- SAP Type
- Customer VID

8 Configure MFIB, STP, and FIB parameters for the site, if required.

i Click on the Forwarding Control tab button. The MFIB tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the site, if required. Otherwise, go to step v.

iv Configure the parameters.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

Note — Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay - 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

v Click on the FIB tab button to configure FIB parameters, if required. Otherwise, go to step 9.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- Move Frequency
- Retry Timeout
- Administrative State

9 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust Count
- Report source address

10 Click on the OK button. The VPLS Site (Create) form closes and a dialog box appears.

11 Click on the OK button. The VPLS Service (Create) form reappears.

12 To create a non-7210 SAS-E or 7210 SAS-D site for the VPLS, perform the following steps.

i Right-click on the Sites icon and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens to display a list of available NEs.

Note 1 — The NE that you choose must be physically connected to the 7210 SAS-E or 7210 SAS-D by a port or LAG.

Note 2 — An NE that is physically connected to a 7210 SAS-E must be exclusively terminating.

ii Choose an NE other than a 7210 SAS-E or 7210 SAS-D and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

iii Configure the site, as described in steps 14 to 36 of Procedure 71-1.

13 Right-click on Access Interfaces below the site and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Description
- Administrative State

Note — If the 7210 SAS-E or 7210 SAS-D sites are connected in a ring network, you must configure an uplink SAP between each pair of 7210 SAS-E or 7210 SAS-D sites.

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - VPLS L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form displays the port information.

18 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Transit SAP

Note — The Outer Encapsulation Value and Inner Encapsulation Value parameters must be configured to values of 0 and *, respectively, in order to configure MSTP on an MVPLS. See Procedure 71-10 for more information.

19 Create an L2 access interface on each 7210 SAS-E or 7210 SAS-D and terminating site. Perform steps 5 to 54 in Procedure 71-3, as required.

Note 1 — Some steps and parameters in Procedure 71-3 are not configurable on a 7210 SAS-D 6F 4T ETR or 7210 SAS-E.

Note 2 — IGMP snooping is not supported for the 7210 SAS-D 6F 4T ETR.

20 Click on the OK button. The VPLS Service (Create) form closes.

Procedure 71-3 To create a VPLS or MVPLS L2 access interface

Perform this procedure to create a VPLS or an MVPLS L2 access interface. Depending on the device type on which you configure an MVPLS, some tabs are not available.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for the creation of a VPLS L2 access interface:

- General
- Port
- Forwarding Control
- Templates
- Faults

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

For information on adding a GNE service interface to a VPLS service, see Procedure 71-15.

5 Right-click on Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- Calling Station ID
- MC Ring Node
- PPPoE Circuit ID

7 On the Split Horizon Group panel, choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - VPLS L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group Name - VPLS L2 Access Interface list form closes, and the VPLS L2 Access Interface (Create) form refreshes with the SHG name.

8 Configure the SAP Sub Type parameter.

Note — When you choose Capture as the SAP Sub Type, the displayed form changes to allow configuration of the Capture SAP. To create a Capture SAP, see Procedure 68-20.

9 Select an application profile for the L2 access interface.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - VPLS L2 Access Interface form closes and VPLS L2 Access Interface (Create) form refreshes with the application profile information.

Note — The Application Profile String: - VPLS L2 Access Interface service form displays only local profiles on the NE.

10 Associate an AA transit prefix policy with the L2 access interface, if required.

Note 1 — To bind a transit policy to an access interface, a port must already exist on the interface.

Note 2 — You can bind a transit policy to only one access interface or spoke SDP binding per node.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit prefix policy and click on the OK button.

11 Configure the parameters in the ETH-CFM MIP panel:

- MIP
- MIP MAC Address

Note — The MIP and MIP MAC Address parameters are configurable only when a port is assigned to the interface.

12 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab button.

13 Perform one of the following:

a Select an operational group for the L2 access interface to join as a member. Go to step 14.

b Select an operational group for the L2 access interface to monitor. Go to step 15.

14 Select an operational group for the L2 access interface to join as a member. Perform the following steps.

i Click on the Select button next to the Member Group Name parameter. The Select Operational Group - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form refreshes with the operational group information.

15 Select an operational group for the L2 access interface to monitor. Perform the following steps.

i Click on the Select button next to the Monitored Group Name parameter. The Select Operational Group - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form refreshes with the operational group information.

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - VPLS L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form displays the port information.

Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

19 If the L2 access interface is on a 7250 SAS-ES or 7250 SAS-ESA, configure the following parameters; otherwise, go to step 21:

- Encapsulation Tagging
- Set Default VLAN to VPLS Tag
- VPLS Mode

The VPLS Mode parameter is configurable on the first L2 access interface associated with a port on the 7250 SAS-ES or 7250 SAS-ESA, Release 3.0 R4 or later.

20 If the L2 access interface is on a 7250 SAS-ES or 7250 SAS-ESA, go to step 52.

21 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

If you are configuring the port for an L2 Access Interface in a Control VPLS for an Ethernet ring, the Outer Encapsulation Value and Inner Encapsulation Value for the port in each L2 Access Interface must have the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively, that you use for the particular path endpoint. This defines the interface as a Control SAP for the Ethernet ring. Refer to Procedure 33-10 for additional information.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only when the port is an ATM port.

If the port you have chosen is an Ethernet port and uses ATM, dot1q or Q in Q encapsulation, you can enable ingress VLAN translation, if required. Configure the parameters:

- Translation
- Translation ID

22 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP or an L2 Access Interface for an Ethernet ring, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

23 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-L2 Access Interface form opens.

ii Choose an EMG and click on the OK button. The Select Egress Multicast Group-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

24 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If you select a bundle in step 18, only the Scheduling Class parameter is configurable.

25 If you are creating this L2 Access Interface for the Control VPLS of an Ethernet ring or for a data service using the ring, configure the ID parameter in the Ethernet Ring Element section to select the required Ethernet Ring Element. Refer to Procedure 33-7 for additional information.

26 Click on the QoS tab button to assign ingress and egress QoS policies to the interface, if required, and perform one of the following:

a To configure a 7450 ESS, 7705 SAR, 7710 SR, or 7750 SR, perform the following steps.

i Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is dot1q, BCP dot1q, or Q in Q.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

ii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPLS L2 Access Interface form opens.

iii Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you choose an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 20-1 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

iv Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPLS L2 Access Interface form opens.

v Choose an egress QoS policy and click on the OK button. The Select Egress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you choose an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 20-1 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

vi If you are configuring an L2 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 18 is not an HSMDA port, then go to step 27.

vii Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

viii Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

ix Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

x Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xi Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

b To configure a 7210 SAS-D 6F 4T ETR, 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP, perform the following steps.

i Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - VPLS L2 Access Interface form opens.

ii Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - VPLS L2 Access Interface form closes and the information is displayed.

Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

iii Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst

Note 1 — The Ingress Meter parameter is configurable only during SAP creation on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP. The parameter must be set to true to support H-metering.

Note 2 — On a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, or 7210 SAS-X 24F 2XFP, the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters are configurable only after SAP creation.

27 Click on the Schedulers tab button to configure scheduling, if required; otherwise, go to step 29.

Note 1 — The Schedulers tab is configurable only when a port is assigned to the interface.

Note 2 — For the 7210 SAS-X, the port is enabled only when you select the SAP based type in the Egress Scheduler Mode.

28 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 18 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 18 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPLS L2 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 18 is an HSMDA port, go to step 29.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPLS L2 Access Interface form opens.

ix Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 29.

b Specify that an access scheduler policy is applied to the interface.

Note — You cannot specify an access scheduler policy if the port you selected in step 18 is an HSMDA port. Go to step 29.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPLS L2 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

29 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - VPLS L2 Access Interface form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - VPLS L2 Access Interface form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - VPLS L2 Access Interface form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

30 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPLS L2 Access Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

v If you are configuring statistics collection for a 7210 SAS-E, go to step vi. Otherwise, go to step 31.

vi Configure the parameters:

- Enable Egress Packets Forwarding
- Ingress Counter Mode

31 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - VPLS L2 Access Interface list form opens.

iii Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - VPLS L2 Access Interface list form closes, and the VPLS L2 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface; you must first disable the Collect Accounting Statistics parameter in step 30.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

32 Configure BPDU Termination, STP and FIB parameters for the interface, if needed.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination
  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface
  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step 33.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The L2 Access Interface (Create) form refreshes with the new MST instance.

33 Configure residential subscriber management for the interface, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step x.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

iv Click on the IGMP Host Tracking tab button.

v Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

vi Configure the filter criteria and click on the Search button. A list of import policies appears.

vii Choose a policy and click on the OK button. The selected import policy name appears.

viii Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group
- Disable Router Alert Check

ix Click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this L2 access interface.

x Click on the Profiles tab button.

xi Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- LAG link selection

xii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the interface, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

xiii Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

xiv Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xv Choose an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xvi Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xvii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xviii Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xix Choose an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xxi Choose a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xxii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xxiii Choose an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xxiv Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxv Choose an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

34 Assign a DoS protection policy to the interface, if required.

> **Note —** A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - VPLS L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - VPLS L2 Access Interface form closes and the policy ID is displayed on the VPLS L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

35 Configure an Ethernet tunnel.

> **Note —** You can only configure Ethernet tunnel SAP path parameters if you are creating a same-fate SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 36.

iii Click on the Create button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The VPLS L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

36 Configure a redundant VLAN range, if required.

> **Note —** If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Create button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VPLS L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

37 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ATM policy name.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ATM policy name.

38 Configure IGMP snooping for the interface, if required.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters as they apply to a specific NE:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Select button in the Mcast CAC panel to choose a multicast CAC policy, if required. The Select Multicast CAC Policy form opens with the list of available multicast CAC policies displayed.

iv Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy form closes and the multicast CAC policy information appears on the VPLS L2 Access Interface (Create) form.

v Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

vi Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 40.

vii Click on the Create button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

viii Configure the parameters:

- Group Address
- Source Address

ix Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xii.

x Click on the OK button.

xi Repeat steps vii to ix to create an additional entry, if required.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

39 Configure the ARP host for the interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)

40 Configure DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State
- Description
- Snooping
- Enable
- Enable Lease Populate
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String

The Enable Lease Populate parameter is configurable when the Enable parameter is enabled.

The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

iii Depending on the type and version of the device that you are configuring, the Subscriber Authentication Policy panel appears. Otherwise, go to step vii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form opens.

v Click on the Search button.

vi Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form closes, and the VPLS L2 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Click on the Server tab button to configure the VPLS L2 access interface proxy server.

Note — You can configure a VPLS L2 access interface proxy server on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7450 ESS, 7710 SR, or 7750 SR.

viii Configure the parameters:

- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

41 Depending on the type of device that you are configuring, the MVR tab is configurable. Configure MVR for the SAP, if required.

i Click on the MVR tab button.

ii Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

iii Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Create) form refreshes with the source MVR VPLS information.

iv Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

v Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Create) form refreshes with the proxy MVR SAP information.

Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

42 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Reply Agent
- MAC Pinning

The ARP Reply Agent parameter is configurable only when an IP address is specified for the static hosts on the SAP.

iii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP. Otherwise, go to step 44.

iv Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

Note — You must specify at least one IP address or MAC address for each static host. The values that are specified for the Anti-Spoofing and ARP Reply Agent parameters determine the type of address entry that is required for the static host. For example, if you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

vi Configure residential subscriber management for the static host, if required. Otherwise, go to step 44.

vii Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step ix.

viii Choose a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

ix Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed. Otherwise, go to step xiii.

x Choose an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

xi Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed. Otherwise, go to step xiii.

xii Choose an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

xiii Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xvi.

xiv Click on the OK button.

xv Repeat steps v to xiv for each additional entry that you want to create.

xvi Click on the OK button. A dialog box appears.

xvii Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes, and the VPLS L2 Access Interface (Create) form refreshes with the new static host entries in a list.

43 Specify the queue overrides.

i Click on the Override Policy Items tab button.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

ii Set the queue overrides, as described in Procedure 47-44.

44 Associate a MEP with the L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

Note — If you have configured a SAP, the SAP information is filled in when you configure the MEP.

45 Enable facility tunnel MEP with the L2 Access interface, if required.

i Click on the General tab button.

ii Right-click Tunnel Fault Notification and select Accept from the contextual menu.

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

46 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

47 Click on the MIPs tab button.

48 Perform one or more of the following, if required:

a Click the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click the Properties button to display the MIP information.

c Click the Resync button to resync the latest MIPs configured on the node.

49 Configure PIM snooping for the interface, if required.

i Click on the PIM Snooping tab button. The General tab is displayed.

ii Configure the Max Number of Groups parameter.

iii Click on the OK button.

50 Configure MLD snooping for the interface, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- MLD version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and MLD version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 51.

iv Click on the Create button. The Access Interface Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

51 Depending on the type of device that you are configuring, the MVR (MLD) tab is configurable. Use the MVR (MLD) tab to use MLD snooping on the SAP. Configure MVR for the SAP, if required.

i Click on the MVR (MLD) tab button.

ii Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

iii Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Create) form refreshes with the source MVR VPLS information.

iv Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

v Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Create) form refreshes with the proxy MVR SAP information.

Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

52 Click on the OK button. The VPLS L2 Access Interface (Create) form closes and a dialog box appears.

53 Click on the OK button. The VPLS (Create) form reappears.

54 Repeat steps 5 to 53 for each additional access interface that you want to create.

55 Click on the OK button. A dialog box appears.

56 Click on the Yes button. The VPLS (Create) form closes.

Procedure 71-4 To create a VPLS mesh SDP binding

The value of the Automatic Mesh SDP Binding Creation parameter determines the way that mesh SDP binding creation occurs in the VPLS.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for the creation of a mesh SDP binding:

- General
- Return
- States
- Frame Sizes
- Forwarding Control
- Templates
- Faults

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the mesh SDP binding; expand the entries for that site.

5 Right-click on Mesh SDP Bindings below the site and choose Create Mesh SDP Binding. The Mesh SDP Binding (Create) form opens with the General tab displayed.

6 If automatic mesh SDP binding creation is enabled on the VPLS, a dialog box appears. The message in the dialog box discourages manual mesh SDP binding creation when automatic mesh SDP binding creation is specified for a VPLS. Perform one of the following.

   a Choose not to override automatic SDP binding creation. Alcatel-Lucent recommends this action.

      i Click on the No button.

      ii Click on the cancel button to abort the operation and close the VPLS management form.

   b Choose to override automatic SDP binding creation. Alcatel-Lucent does not recommend this action.

      i Click on the Yes button. The Mesh SDP Binding (Create) form opens.

      ii Consult an Alcatel-Lucent technical representative before proceeding.

7 Specify a destination node for the mesh SDP binding:

   a If the destination node is a managed node, choose from a list of managed nodes.

      i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Mesh SDP Binding form opens.

      ii Select a destination node and click on the OK button. The Select Destination Network Element - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

   b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

8 Configure the parameters:

- Description
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

9 Perform one of the following to specify a transport tunnel for the mesh SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Configure the parameters:

- Egress Label
- Enable Hash Label
- Enable Signal Capability
- Force VLAN VC Forwarding

Note — The Force VLAN VC Forwarding parameter does not appear if you are creating a Mesh SDP binding for a B-site.

11 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Mesh SDP Binding form opens.

iii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

12 Specify whether the mesh SDP binding is in or out of service.

i Click on the States tab button.

ii Configure the Administrative State parameter.

13 Click on the Pseudowire OAM tab button.

14 Configure the Control Word parameter.

15 Assign ingress and egress ACL filters to the mesh SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Mesh SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Mesh SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Mesh SDP Binding form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Mesh SDP Binding form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

16 Configure anti-spoofing for the mesh SDP binding, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

17 Assign an accounting policy to the mesh SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Mesh SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the accounting policy name.

18 Click on the Forwarding Control tab button if you need to add or delete MFIB allowed daughter cards or configure MRP, otherwise go to step 19.

Note 1 — The single-slot models of the 7450 ESS and 7750 SR support the addition or deletion of MFIB allowed daughter cards.

Note 2 — The MFIB Allowed Daughter Card tab does not appear if you are creating a Mesh SDP binding for a B-site.

i Click on the MFIB Allowed Daughter Card tab button.

ii Click on the Create button. The SDP Binding MFIB Allowed Daughter Card (Create) form opens.

iii Click on the Select button. The Select Daughter Card form opens. Select a daughter card and click OK. The Select Daughter Card form closes.

iv Click on the OK button. The SDP Binding MFIB Allowed Daughter Card (Create) form closes and a dialog box appears.

v Click on the OK button. The Mesh SDP Binding (Create) form displays the new allowed daughter card in the list.

vi Click on the MRP tab if you are configuring a Mesh SDP binding for a B-site.

vii Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave All Time (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

viii Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

ix Choose the desired policy and click OK.

19 Configure DHCP for the mesh SDP binding, if required.

i Click on the DHCP tab button.

Note — The DHCP tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Description
- Snooping

20 Configure IGMP Snooping for the mesh SDP binding, if required.

i Click on the IGMP Snooping tab button.

Note — The IGMP Snooping tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

iii Configure a multicast CAC policy, if required. Otherwise, go to step 23.

iv Click on the Select button. The Select Multicast CAC Policy form opens.

v Select a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy form closes.

vi Click on the Properties button to edit the existing multicast CAC policy, if required. See chapter 49 for information about creating a multicast CAC policy.

vii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

21 Associate a MEP with the mesh SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

22 Configure MLD Snooping for the mesh SDP binding, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

Note — The MLD Snooping tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- MLD version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and MLD version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 23.

iv Click on the Create button. The Circuit Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

23 Click on the OK button. The Mesh SDP Binding (Create) form closes, and a dialog box appears.

24 Click on the OK button. The VPLS (Edit) form reappears.

25 Repeat steps 5 to 24 for each additional mesh SDP binding that you want to create.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button. The VPLS (Edit) form closes.

28 Close the Manage Services form.

Procedure 71-5 To create a VPLS spoke SDP binding

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP. Likewise, you cannot enable MSTP for a site that has a spoke SDP binding, or on a SAP with a non-zero encapsulation value.

Note 2 — For services employing BGP AD and BGP VPLS: You should create SDP bindings manually at non-BGP AD or BGP VPLS enabled sites, or to other BGP AD or BGP VPLS sites where auto-created pseudowires are not expected to be created.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 If you are creating a redundant spoke SDP binding under an endpoint, go to step 5. Otherwise go to step 8.

Note — Redundant spoke SDP bindings under an endpoint are only valid for VPLS regular sites and B-Sites. They do not apply to I-Sites.

5 On the navigation tree, click on the site where you want to create a redundant spoke SDP binding under an endpoint; expand the entries for that site.

6 Select an endpoint for the required site.

7 Right-click on Spoke SDP Bindings below the endpoint and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed. Go to step 10.

8 On the navigation tree, click on the site where you want to create a VPLS spoke SDP binding; expand the entries for that site.

9 Right-click on Spoke SDP Bindings below the site and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

10 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Select a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

11 Configure the parameters:

- Description
- Auto-Assign ID
- VC ID
- VC Type
- MTU
- VLAN VC Tag
- Ingress Label
- Egress Label

Note — The MTU parameter does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

12 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note 1 — If you are creating a Spoke SDP binding for a B-site, the Tunnel Auto-Selection Transport Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

Note 2 — The Auto-Select Transport Tunnel parameter supports only values of Any or MPLS:RSVP on a Spoke SDP binding that originates from 7250 SAS-ES or 7250 SAS-ESA sites.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

13 Perform one of the following:

a Select an operational group for the Spoke SDP Binding to join as a member. Go to step 14.

b Select an operational group for the Spoke SDP Binding to monitor. Go to step 15.

14 Select an operational group for the Spoke SDP Binding to join as a member. Perform the following steps.

i Click on the Select button next to the Member Group Name parameter. The Select Operational Group - VPLS Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the operational group information.

15 Select an operational group for the Spoke SDP Binding to monitor. Perform the following steps.

i Click on the Select button next to the Monitored Group Name parameter. The Select Operational Group - VPLS Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - VPLS Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the operational group information.

16 If you are creating the spoke SDP binding for a B-Site or an I-Site, go to step 21.

17 If you are configuring a spoke SDP binding that originates from a 7250 SAS-ES or 7250 SAS-ESA perform the following steps:

i Configure the Active State parameter.

ii Go to step 41.

18 If you are creating the spoke SDP binding under an endpoint, go to step 20.

19 Click on the Select button in the Redundancy panel to select the desired endpoint from the drop-down menu.

20 Configure the parameters:

- Ignore Standby Signalling
- Precedence

21 Choose an SHG for the spoke SDP binding, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - Spoke SDP Binding form opens.

Note — You must configure an SHG or residential SHG on a spoke SDP binding for an HVPLS that includes another VPLS or a VLL service.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the SHG name.

22 Configure the parameters:

- Enable Hash Label
- Enable Signal Capability
- Enable PW Status Signaling
- Force VLAN VC Forwarding
- MIP

Note — The Force VLAN VC Forwarding parameter do not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

23 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — If you are creating a Return SDP binding for a B-site, the Return Tunnel Auto-Selection Transport Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

24 Select an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an Application Profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPLS service form displays only local profiles on the NE.

25 Associate an AA transit prefix policy with the spoke SDP binding, if required.

Note 1 — You can bind a transit policy to only one access interface or spoke SDP binding per node.

Note 2 — The transit policy and the application profile must belong to the same application assurance group or partition.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit prefix policy and click on the OK button.

26 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Name
- Subscriber Class
- Subscriber Type
- Total Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Downstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

27 Specify whether the spoke SDP binding is in or out of service.

- **i** Click on the States tab button.
- **ii** Configure the Administrative State parameter.
- **iii** Configure the Block On Mesh Failure parameter.

Note — The Block On Mesh Failure parameter does not appear if you are creating a Spoke SDP binding for a B-site or an I-site.

28 Click on the Pseudowire OAM tab button.

29 Configure the Control Word parameter.

30 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

- **i** Click on the ACL tab button.
- **ii** Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.
- **iii** Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the ingress ACL filter name.
- **iv** Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.
- **v** Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the egress ACL filter name.
- **vi** Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.
- **vii** Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.
- **viii** Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.
- **ix** Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

31 Configure anti-spoofing for the spoke SDP binding, if required.

- **i** Click on the Anti-Spoofing tab button.
- **ii** Configure the MAC Pinning parameter.

32 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the accounting policy name.

33 Configure BPDU Termination, STP, FIB, MRP, and MFIB Allowed Daughter Card parameters for the spoke SDP binding, if required.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU tab is displayed.

ii Configure the parameters:

- L2 Protocol Termination
- BPDU Translation

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source

Note — The Maximum Entries parameter does not appear if you are creating a Spoke SDP binding for a B-site.

vii Click on the MFIB Allowed Daughter Card tab button to configure allowed daughter cards; otherwise, go to step 34.

Note 1 — The MFIB Allowed Daughter Card tab does not appear if you are creating a Spoke SDP binding for a B-Site.

Note 2 — The single-slot models of the 7450 ESS and 7750 SR support the addition or deletion of MFIB allowed daughter cards.

viii Click on the Create button. The SDP Binding MFIB Allowed Daughter Card (Create) form opens.

ix Click on the Select button. The Select Daughter Card form opens.

x Select a daughter card in the list and click on the OK button. The Select Daughter Card form closes.

xi Click on the OK button. The SDP Binding MFIB Allowed Daughter Card (Create) form closes and the MFIB Allowed Daughter Card tab displays the newly-added daughter card in the list.

xii Click on the MRP tab if you are configuring a Spoke SDP binding for a B-site.

Note — The MRP tab does not appear if you are creating a Spoke SDP binding for an I-site.

xiii Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave All Time (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

xiv Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

xv Choose the desired policy and click OK.

34 Configure IGMP Snooping for the spoke SDP binding, if required.

Note — The IGMP Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

iii If you are creating this spoke SDP binding for a B-Site or an I-Site, go to step viii.

iv Configure a multicast CAC policy, if required. Otherwise, go to step 35.

v Click on the Select button. The Select Multicast CAC Policy form opens.

vi Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy form closes.

vii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

viii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 35.

ix Click on the Create button. The Circuit Igmp Snooping Mcast Group Display (Create) form opens.

x Configure the parameters:

- Group Address
- Source Address

xi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xiv.

xii Click on the OK button.

xiii Repeat steps x to xii to create additional entries, if required.

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

35 Configure DHCP for the spoke SDP binding, if required.

Note — The DHCP tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

i Click on the DHCP tab button.

ii Configure the parameters:

- Description
- Snooping

36 Associate a MEP with the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

37 Click on the MIPs tab button.

38 Perform one or more of the following, if required:

a Click the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click the Properties button to display the MIP information.

c Click the Resync button to resync the latest MIPs configured on the node.

39 Configure PIM snooping for the spoke SDP binding, if required.

i Click on the PIM Snooping tab button. The General tab is displayed.

Note — The PIM Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

ii Configure the Max Number of Groups parameter.

iii Click on the OK button.

40 Configure MLD Snooping for the spoke SDP binding, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

Note — The MLD Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Disable Router Alert Check
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- MLD version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and MLD version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 35.

iv Click on the Create button. The Circuit Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

41 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

42 Click on the OK button. The VPLS (Edit) form reappears.

43 Repeat steps 9 to 42 for each additional spoke SDP binding that you want to create.

44 Click on the OK button. A dialog box appears.

45 Click on the Yes button. The VPLS (Edit) form closes.

46 Close the Manage Services form.

Procedure 71-6 To configure a site for BGP AD or BGP VPLS

This procedure provides the steps required to enable BGP Auto Discovery or configure BGP VPLS on a VPLS site.

- BGP AD enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. T-LDP based label signaling is used for the pseudowire.
- BGP VPLS provides the mechanism for service member auto-discovery based on Route Target. MP-BGP based label signaling is used for the pseudowire.

Note 1 — This procedure can only be performed for an existing site, not during the creation of a new site.

Note 2 — BGP AD and BGP VPLS implementations only apply to regular VPLS sites and B-Sites, but not to I-Sites. For BGP VPLS, the B-Site cannot be used as a backbone for an I-Site or Epipe.

1 Prior to configuring a site for BGP AD or BGP VPLS, you must complete the following actions:

a Create a routing policy to define the required community members. See Procedure 30-11. This defines the VSI Import/Export Routing Targets.

b Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 31-1 for more information.

c Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 31-2 for more information. The following items are required for BGP AD implementation.

- On the VPN tab of the Routing Instance form, you must enable the L2 VPN parameter in the Family block and in the Rapid Update Address Family block.
- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.

d Create a PW template. See chapter 58 for information about PW templates.

e Distribute the PW Template to each NE that is or will be a component of the VPLS or BGP VPLS.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria. A list of services appears.

4 Select a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

6 Click on the BGP tab button.

7 Configure the Route Distinguisher parameter.

8 Click the Configuration button to configure the Route Targets and the PW Templates. The BGP Configuration form opens, with the VSI Import Policies tab displayed.

a Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

b Perform one of the following:

i Enter the Import Route Target name manually in the provided field. The format be “target:x:y”.

ii Click on the Import Route Target Select button. The Select ...-BGP Info form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select ...-BGP Info form closes.

c Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

d Perform one of the following:

i Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

ii Click on the Export Route Target Select button. The Select ...-BGP Info form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select ...-BGP Info form closes.

e Click on the PW Template Binding tab button.

f Perform one of the following:

i To use an existing PW Template Binding, go to step g.

ii To add a new PW Template Binding, go to step h.

g For an existing PW Template Binding:

i Click the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step i.

h To create a new PW Template Binding:

i Click the Create button. The PW Template Binding (Create) form opens with the General tab displayed.

ii Enter a Split Horizon Group name, if required.

iii Click the Select button. The Select PW Template form is displayed.

iv Click the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click OK to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the Select button next to the Member Group Name parameter. The Select Operational Group - PW Template Binding form opens.

viii Configure the filter criteria. A list of operational groups appears.

ix Choose an operational group from the list and click on the OK button. The Select Operational Group - PW Template Binding form closes and the PW Template Binding (Create) form refreshes with the operational group information.

x Click on the PW Templates Binding Route Target tab and click the Create button. The PW Template Binding Route Target (Create) form is displayed.

Note — This Import Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Import Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Import Route Target is displayed in the table on the PW Template Binding Route Target tab.

xi Click OK to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

xii Repeat steps i to xi to create additional PW Template Bindings, as required.

xiii Select the required entry or entries from the list.

i Click the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

9 If you are configuring a BGP VPLS, go to step 10. Otherwise go to step 13.

10 Enable the Enable BGP VPLS parameter. The BGP VPLS section is displayed.

11 Configure the parameters:

- VE Name
- Max VE ID
- VE ID
- Administrative State

12 Select an operational group for the BGP site to monitor. Perform the following steps.

i Click on the Select button next to the Monitored Group Name parameter. The Select Operational Group - BGP Multi-homing VPLS site form opens.

ii Configure the filter criteria. A list of operational groups appears.

iii Choose an operational group from the list and click on the OK button. The Select Operational Group - BGP Multi-homing VPLS site form closes and the BGP Multi-homing VPLS site (Create) form refreshes with the operational group information.

13 If you are configuring BGP AD, go to step 14. Otherwise go to step 17.

14 Enable the Enable BGP AD parameter. The BGP AD section is displayed.

15 Configure the parameters:

- VPLS ID
- Formatted VSI ID Prefix
- Administrative State

Note 1 — The Global Service VPLS ID is set to the value defined at the service level.

Note 2 — If VPLS ID is defined at the service level, then the 5620 SAM ensures that each site has the same VPLS ID. If a site has a different VPLS ID, an alarm is raised and the ID mismatch is indicated in the Status panel of the VPLS site properties form.

The same VPLS ID value is propagated to each site in a VPLS. If you change the VPLS ID of a site without using the 5620 SAM, the 5620 SAM displays a warning form.

16 Click on the OK button. The VPLS Site (Edit) form closes.

17 Click on the OK button. A dialog box appears.

18 Close the VPLS Service (Edit) form.

Procedure 71-7 To configure a site for BGP VPLS Multi-homing

This procedure provides the steps required to configure a site for BGP VPLS Multi-homing.

BGP VPLS Multi-homing provides redundancy support through the configuration of a number of multi-homed sites, rather than through the use of MC-LAG or MC-Ring as access mechanisms. Dual-homing between a CE device and a pair of VPLS PE devices (potentially in different autonomous systems) is an example of such a configuration.

Note 1 — This procedure can only be performed for an existing site, not during the creation of a new site.

Note 2 — Only regular VPLS sites and B-Sites can be configured for BGP VPLS Multi-homing. However, the B-Sites cannot be used as a backbone for an I-Site or Epipe.

Note 3 — I-VPLS and MVPLS services cannot be configured for this application.

Note 4 — An RD or RT configured under the BGP of a VPLS site cannot be removed as long as there is a multi-homing site ID configured whose administration state is up.

Note 5 — You can see a list of all current BGP VPLS Multi-homing sites in a multi-homing VPLS service by viewing the BGP Multi-homing Sites tab on the service configuration form.

1 Prior to configuring a site for BGP VPLS Multi-homing, you must complete the following actions:

a Create a routing policy to define the required community members. See Procedure 30-11. This defines the VSI Import/Export Routing Targets.

b Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 31-1 for more information.

c Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 31-2 for more information. The following items are required:

- On the VPN tab of the Routing Instance form, you must enable the L2 VPN parameter in the Family block.

Note — For optimal processing while a BGP multi-homing site is activated or de-activated, or the system is rebooted, you should also:

- Enable the L2 VPN parameter in the Rapid Update Address Family block on the BGP site's VPN tab.
- Enable the Enable Rapid Withdrawal parameter on the BGP site's Behavior tab.

- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.

d Create a PW template. See chapter 58 for information about PW templates.

e Distribute the PW Template to each NE that is or will be a component of the VPLS or BGP VPLS.

f Create SDPs for the BGP VPLS Multi-homing site(s), if manually-provisioned service tunnels are required. Refer to Procedure 33-1.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria. A list of services appears.

4 Select the required VPLS or HVPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

6 Click on the BGP tab button. The General sub-tab is displayed.

7 Configure the Route Distinguisher parameter.

8 Click the Configuration button to configure the Route Targets and the PW Templates. The BGP Configuration form opens, with the VSI Import Policies tab displayed.

  a Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

  b Perform one of the following:

    i Enter the Import Route Target name manually in the provided field. The format must be “target:x:y”.

    ii Click on the Import Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

  c Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

  d Perform one of the following:

    i Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

    ii Click on the Export Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

  e Click on the PW Template Binding tab button.

  f Perform one of the following:

    i To use an existing PW Template Binding, go to step g.

    ii To create a new PW Template Binding, go to step h.

g For an existing PW Template Binding:

i Click the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step i.

h To create a new PW Template Binding:

i Click the Create button. The PW Template Binding (Create) form opens with the General tab displayed.

ii Enter a Split Horizon Group name, if required.

iii Click the Select button. The Select PW Template form is displayed.

iv Click the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click OK to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the PW Templates Binding Route Target tab and click the Create button. The PW Template Binding Route Target (Create) form is displayed.

Note — This Import Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Import Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Import Route Target is displayed in the table on the PW Template Binding Route Target tab.

viii Click OK to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

ix Repeat steps i to viii to create additional PW Template Bindings, as required.

x Select the required entry or entries from the list.

i Click the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

9 Click on the Multi-homing sub-tab button.

10 Click on the Create button. The BGP Multi-homing VPLS Site (Create) form opens.

11 Configure the parameters:

- Multi-homing Site Name
- Multi-homing ID
- Enable Multi-homing to

12 Click the Select button to specify a SAP, Spoke SDP, or a Split Horizon Group, based on the option you selected for the Enable Multi-homing to parameter.

13 Configure the parameters:

- Failed Threshold
- Use Node Level Boot Timer
- Boot Timer (seconds)
- Use Node Level Site Activation Timer
- Activation Timer (seconds)
- Administrative State

If you enable either the Use Node Level Boot Timer and/or Use Node Level Site Activation Timer parameters, then the associated Boot Timer (seconds) and/or Activation Timer (seconds) parameters will not be configurable. These parameter values will be inherited from the network element configuration.

The Boot Timer (seconds) and Activation Timer (seconds) parameters can be configured for an NE on the BGP Multi-homing sub-tab under the Redundancy tab in the Network Element (Edit) form. See Procedure 17-2 for more information on changing device properties.

14 Click on the Apply button. A dialog box appears.

15 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form refreshes.

16 Check the following indicators:

- Operational State: indicates the operational status of the multi-homing site.
- Designated Forwarder: indicates whether this site has been declared as designated forwarder, depending on the result of the BGP election.

17 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form closes.

18 Click on the OK button. The VPLS Site (Edit) form closes.

19 Close the VPLS Service (Edit) form.

Procedure 71-8 To re-evaluate the PW Templates associated with a BGP AD or BGP VPLS

Use this procedure to re-evaluate changes made to the Route Targets associated with the PW Template bindings of an existing site with BGP configuration. This procedure can only be performed on an existing VPLS that has been configured with BGP AD or BGP VPLS. The procedure allows you to make configuration changes and propagate them to the service without having to shutdown and then turn up a site.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

5 Click on the BGP tab button.

6 Click the Configuration button to open the BGP Configuration form.

7 Make any required changes to the Route Targets or PW Template bindings. Refer to Procedures 71-6 or 71-7 as required, for detailed instructions on configuring these items.

8 Click the PW Template Binding tab and click the Apply button to apply the changes you have made.

9 Perform one of the following:

- **i** If you need to update the PW Templates under other sites for this service, repeat steps 4 to 8 as required, then go to step 13.
- **ii** If you do not need to update the PW Templates under other sites for this service go to step 10.

10 Click the Re-evaluate PW Template button to run an evaluation of the PW Template bindings. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

If you make any subsequent modifications, you can re-evaluate the template again.

11 Click OK. The BGP Configuration form closes.

12 Click the OK button to close the VPLS Service (Edit) form. The procedure is complete.

13 Return to the VPLS (Edit) form.

14 Click the Re-evaluate PW Template button. The Add form opens to allow you to select one of the PW Templates you modified.

15 Click the Search button to display a list of PW Templates and select the required one.

16 Click the OK button to run an evaluation of the selected PW Template. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

17 Repeat steps 14 to 16 for any other sites that you want to re-evaluate a PW Template for.

18 Click the OK button to close the VPLS Service (Edit) form.

Procedure 71-9 To create an HVPLS

Perform this procedure to create an HVPLS. An HVPLS consists of a VPLS in which one or more sites connect to other sites in the same VPLS, different VPLS, or to VLL services.

Note — One VPLS site in an HVPLS must be configured with an SHG. See "Split horizon groups" in this chapter for more information.

1 Add a VPLS to the HVPLS.

a Create a new VPLS.

i Perform Procedure 71-1.

Caution — If you are creating an HVPLS that includes two sites in the same VPLS connected by spoke SDPs, do not create mesh SDP bindings between the sites. Mesh SDP binding functionality is available in the spoke SDP bindings between the sites.

ii Go to step 2.

b Use an existing VPLS. Go to step 3.

2 Create another service for inclusion in the HVPLS, if required.

a Create a VPLS.

i Perform Procedure 71-1.

ii Go to step 3.

b Create a VLL.

i Perform the appropriate VLL creation procedure in chapter 70.

ii Go to step 3.

3 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with the General tab displayed.

4 Configure the filter criteria. A list of services appears.

5 Select a VPLS that you want to include in the HVPLS and click on the OK button. The VPLS (Edit) form opens.

6 Right-click on Spoke SDP Bindings below the site and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

7 Perform Procedure 71-5 beginning with step 10. Choose the destination node for the site that you want to include in the HVPLS as the Tunnel Termination Site.

8 Perform this procedure as required to add sites to the HVPLS.

Procedure 71-10 To create an MVPLS

An MVPLS runs RSTP or MSTP to manage traffic blocking on the associated VPLS. Perform this procedure to create an MVPLS to run MSTP, or to run RSTP and manage traffic on the associated VPLS SAPs or redundant spoke SDPs. The procedure also applies to the I-Sites and B-Sites used in PBB.

1 Choose Create→Service→MVPLS from the 5620 SAM main menu. The MVPLS (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the MVPLS. The Select Customer - MVPLS form opens.

3 Select a customer for the MVPLS and click on the OK button. The Select Customer - MVPLS form closes, and the MVPLS (Create) form refreshes with the customer name.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Default Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Per Service Hashing for LAG Enabled
- OLC State
  This parameter is configurable when you click on the Apply button.

5 On the navigation tree, right-click on Sites under MVPLS and choose one of the following, as required:

- Create MVPLS B-Site
- Create MVPLS I-Site
- Create MVPLS Site

The Select Network Elements - MVPLS form opens with a list of available sites.

6 Select a site and click on the OK button. Depending on your selection in step 5, the MVPLS B-Site (Create), MVPLS I-Site (Create), or MVPLS Site (Create) form opens with the General tab displayed.

7 Perform one of the following:

a Create an RSTP site for the MVPLS.

i For regular VPLS sites, perform steps 14 to 35 of Procedure 71-1. Specify RSTP as the value for the STP Mode parameter in step 16. Go to step iv when completed.

ii For B-Sites, perform steps 8 to 20 of Procedure 71-11. Specify RSTP as the value for the STP Mode parameter in step 11iv. Go to step iv when completed.

iii For I-Sites, perform steps 8 to 19 of Procedure 71-12. Specify RSTP as the value for the STP Mode parameter in step 12 iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

b Create an MSTP site for the MVPLS.

Note — MSTP is configurable only on the 7210 SAS-D, 7210 SAS-E, 7450 ESS, and 7750 SR.

i For regular VPLS sites, perform steps 14 to 35 of Procedure 71-1. Specify MSTP as the value for the STP Mode parameter in step 16. Go to step iv when completed.

ii For B-Sites, perform steps 8 to 20 of Procedure 71-11. Specify MSTP as the value for the STP Mode parameter in step 11iv. Go to step iv when completed.

iii For I-Sites, perform steps 8 to 19 of Procedure 71-12. Specify MSTP as the value for the STP Mode parameter in step 12iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

8 Click on the OK button. The MVPLS (Create) form reappears.

9 If the MVPLS site is to manage traffic on associated VPLS SAPs, create a SAP for the MVPLS with a defined redundant VLAN range.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation in the MVPLS.

- **i** For regular VPLS sites, perform steps 5 to 52 of Procedure 71-3. Ensure that you perform step 36 to specify a redundant VLAN range. Go to step iv when completed.
- **ii** For B-Sites, perform steps 5 to 27 of Procedure 71-13. Ensure that you perform step 22 to specify a redundant VLAN range. Go to step iv when completed.
- **iii** For I-Sites, perform steps 5 to 30 of Procedure 71-14. Ensure that you perform step 24 to specify a redundant VLAN range. Go to step iv when completed.
- **iv** Click on the OK button. The MVPLS (Create) form reappears.

10 Click on the OK button. The MVPLS (Create) form closes.

Procedure 71-11 To create a B-site for VPLS or MVPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS service form opens.

3 Select a customer for the VPLS and click on the OK button. The Select Customer - VPLS service form closes, and the VPLS service (Create) form displays the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Default Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation
- Profile Name
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Perform one of the following.

a Create a B-site for the VPLS. Go to step 6.

b Complete service creation if B-sites, B-L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 23.

6 On the navigation tree, right-click on the Sites icon and choose Create VPLS B-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

7 Select a site and click on the OK button. The B-Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- Default Mesh VC ID
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled

9 Click on the Backbone tab button.

10 Configure the backbone parameters:

- Source MAC Address
- Use SAP Backbone MAC Address
- Administrative State
- MAC Notification Interval (seconds)
- MAC Notification Count

Note 1 — The Source MAC Address should not be duplicated for other B-sites within the same B-VPLS.

Note 2 — The Source MAC Address parameter is the only applicable parameter when configuring PBB on a 7210 SAS-M or a 7210 SAS-X.

Note 3 — The Use SAP Backbone MAC Address parameter is configurable only on the 7750 SR, 7750 SR-c12, or 7450 ESS. The NE must also be configured with an IOM 3 MDA.

11 Configure MFIB, STP, FIB, and MRP parameters for the B-site, if required.

i Click on the Forwarding Control tab button. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the B-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the B-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 1 — If you are configuring an MVPLS B-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 71-10 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab button to configure FIB parameters for the B-site, if required. Otherwise, go to step 12.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on fail
- Propagate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number Of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii If you are configuring an MVPLS B-site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 12.

Note — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

ix Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

x Click on the MST Instances tab button.

xi Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

xii Configure the parameters:

- Instance Index
- Priority

xiii Click on the VLAN Ranges tab button. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

xiv Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xv Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xvi Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xvii Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xviii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

xix Click on the MRP tab button.

xx Configure the parameters:

- MRP Admin Status
- MRP Max Attributes
- MRP Flood Time (seconds)
- MRP Attribute-Table-Low-Watermark
- MRP Attribute-Table-High-Watermark
- MMRP Endstation Only

Note — You can view information regarding MMRP Entries for the access interface and/or SDP Binding by clicking on the MMRP Entries tab button.

12 Create an endpoint for redundancy (dual homing) on the B-site, if required.

i Click on the Endpoints tab button.

ii Click on the Create button. The Endpoint (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- Revert Time (seconds)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Endpoint (Create) form closes and the B-Site (Create) form reappears with the new endpoint displayed in the list.

13 If you are configuring an MVPLS B-site, go to step 17.

14 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS B-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

Note — You can view information about the I-Sites and Epipe sites associated with the B-Site by clicking on the Associated Sites tab button.

15 To create a B-L2 access interface for the site, perform steps 5 to 29 of Procedure 71-13.

16 To create a mesh SDP binding for the site, perform steps 5 to 25 of Procedure 71-4.

17 To create a redundant spoke SDP binding under an endpoint, perform steps 4 to 43 of Procedure 71-5.

18 To create a spoke SDP binding for the site, perform steps 7 to 43 of Procedure 71-5.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

19 Create a virtual MEP on the site, if required. For more information about virtual MEPs, see chapter 46.

i Click on the Virtual MEP tab button.

ii Click on the Create button. The MEP (Create) form opens.

iii Click on the Select button. The Select Maintenance Entity Group form opens.

iv Choose a MEG from the list.

Note — The B-VPLS site must be added to the MEG during MEG configuration. Otherwise, the virtual MEP cannot be created on the B-site. See chapter 38 for more information.

v Configure the parameters:

- Auto-Assign ID
- ID
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi Click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

vii Click on the OK button. The MEP (Create) form closes, and the virtual MEP is created on the B-VPLS site.

20 Click on the OK button. The B-Site (Create) form closes, and a dialog box appears.

21 Click on the OK button. The VPLS (Create) form displays the new site on the navigation tree under VPLS.

22 Repeat steps 6 to 21 to create additional sites for the B-VPLS.

23 Click on the OK button. The VPLS (Create) form closes.

24 Close the Manage Services form.

Procedure 71-12 To create an I-VPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Select a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes, and the VPLS Service (Create) form displays the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Default Service Priority
- Administrative State
- Default Mesh VC ID
  This parameter is configurable when the Inherit Service ID Value parameter is disabled.
- Inherit Service ID Value
- Automatic Mesh SDP Binding Creation
- Profile Name
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.
- Transport Type
  This parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled and the Profile Name parameter is left blank.
- OLC State
  This parameter is configurable when you click on the Apply button.

5 Perform one of the following.

a Create an I-site for the VPLS. Go to step 6.

b Complete service creation if I-sites, I-L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 24.

6 On the navigation tree, right-click on Sites and choose Create VPLS I-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

7 Select a site and click on the OK button. The I-Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the facility tunnel MEP.

9 Click on the Backbone tab button.

10 Select the Backbone VPLS site.

i Click on the Select button. The Select Backbone VPLS Site - I-Site form is displayed.

ii Click the Search button. A list with all the B-VPLSs that can be used by the I-VPLS is displayed. You can narrow the search by using the using the filtered properties shown in the form. Only B-VPLSs that are present in PEs that have the I-Sites of the VPLS is shown.

iii Select a B-VPLS and click on OK. The Select Backbone VPLS Site - I-Site form closes and the Service ID of the chosen B-VPLS appears on the I-Site (Create) form.

Note — The selection of the B-site in this step must be repeated for each I-site you create, since you must select the B-VPLS site that is within the same site as the I-site.

11 Configure the parameters:

- Send Flush All From Me
- Send Flush All But Mine
- Administrative ISID
- Backbone STP
- Force Q Tag Forwarding

Note 1 — The Force Q Tag Forwarding parameter is only displayed if the NE for this site is in chassis mode D or higher or Sparrow.

Note 2 — Only the Administrative ISID and Backbone STP parameters are applicable when configuring PBB on a 7210 SAS-M or a 7210 SAS-X.

12 Configure MFib, STP, FIB, and MAC Protection parameters for the I-site, if required.

i Click on the Forwarding Control tab button. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the I-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the I-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 1 — If you are configuring an MVPLS I-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 71-10 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab button to configure FIB parameters for the I-site, if required. Otherwise, go to step 16.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on fail
- Propagate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number Of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii Click on the MAC Protection tab to configure the list of protected MAC addresses.

ix Click on the Create button. The MAC Protection (Create) form opens.

x Configure the Protected Mac Address parameter.

xi Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

xii If you are configuring an MVPLS I-site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 15.

Note — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

xiii Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

xiv Click on the MST Instances tab button.

xv Click on the Create button. The MST Instance (Create) form opens with the General tab displayed.

xvi Configure the parameters:

- Instance Index
- Priority

xvii Click on the VLAN Ranges tab button. Click on the Create button. The MST Instance Managed VLAN range (Create) form opens.

xviii Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xix Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xx Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xxi Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xxii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

13 Configure ingress multicast forwarding, if required.

Note — An Operational Channels tab appears when you access the VPLS I-Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 46 for information about listing the operational channel parameters.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy form opens.

iii Select a policy in the list and click on the OK button. The Select Ingress Info Policy form closes and the policy identifier is displayed on the Site (Create) form.

14 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust Count
- Report source address
- Use query source address
- Query source address

The Query source address parameter is configurable when the Use query source address parameter is enabled.

15 If you are configuring an MVPLS I-site, go to step 17.

16 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS I-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Create button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

17 To create an I-L2 access interface for the I-site, perform steps 4 to 32 of Procedure 71-14.

18 To create a spoke SDP binding between the I-site and regular VPLS sites, click on the Components tab and perform steps 9 to 43 of Procedure 71-5, as required. I-sites can only use spoke SDP bindings.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on an access interface that has a non-zero encapsulation value.

19 Click on the OK button. The I-Site (Create) form closes, and a dialog box appears.

20 Click on the OK button. The VPLS (Create) form displays the new I-site on the navigation tree under VPLS.

21 Repeat steps 6 to 20 to create additional I-sites for the I-VPLS.

22 Add protected MAC addresses at the service level, if required. Protected MAC addresses that you add on the site level, as performed in step 12, are automatically added to the service-level MAC protection list.

i Click on the Forwarding Control tab button.

ii Click on the MAC Protection tab button.

iii Click on the Create button. The MAC Protection (Create) form opens.

iv Configure the Protected Mac Address parameter.

v Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS (Create) form.

23 To configure bandwidth for the service if required, click on the Bandwidth tab. The Required Bandwidth sub-tab is displayed. Proceed as follows:

Note 1 — The Bandwidth tab is only available if service CAC is configured; see chapter 6 for information about enabling and disabling service CAC.

Note 2 — The ability to configure required bandwidth is only applicable to l-sites.

i For each CoS, enter the value for the CoS Bandwidth (Mbps), as required.

ii Click on the General tab to determine the CAC status.

If the Verify CAC button is enabled, the CAC has not been verified. The Probable Cause and CAC Status fields provide details.

The CAC Status field describes the current CAC status of the service. CAC statuses are as follows.

- CAC Verified indicates that all tunnels have sufficient bandwidth to admit service and that requested bandwidth for the service is booked on the appropriate physical links.
- CAC Failed indicates that the attempt made to admit service into the network was unsuccessful. The most likely cause for this is insufficient bandwidth. See the Probable Cause field for more specific information.
- BW Defined, No CAC Request indicates that the required bandwidth is defined on the service; however, a CAC request has not occurred.
- CAC To be Verified indicates that a tunnel has been configured on the service either manually or through the CLI; however, the required bandwidth has not been verified in the network.

The Probable Cause field describes possible reasons for the current CAC state. Probable causes are as follows.

- No Candidate Tunnels Found indicates that the autobind tunnel function was found, but no suitable tunnels were found.
- Different PBB Tunnels Applied to Service indicates that two or more different PBB tunnels are configured on this service.
- Not Enough Bandwidth on any Candidate Tunnels indicates that one or more candidate tunnels were found, but the available bandwidth was insufficient to admit the service.
- Automatic PBB Tunnel Selection Failed indicates that a suitable PBB tunnel was found, but there were errors when attempting to assign the tunnel to the service. A dialog box will provide more details.
- Site Missing Tunnel indicates that at least one selected site is not configured with a PBB tunnel.
- All PBB Tunnels have not been Verified indicates that all sites within the service have a tunnel configured, but the available bandwidth has not been booked or verified in the network.

iii To manually verify the CAC, click on the Verify CAC button if it is enabled. The 5620 SAM will attempt to find the most appropriate PBB tunnel for the service based on available bandwidth, and to automatically bind the tunnel to the service if one has not already been assigned.

24 Click on the OK button. The VPLS (Create) form closes.

25 Close the Manage Services form.

Procedure 71-13 To create a VPLS or MVPLS B-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

5 Right-click on Access Interfaces and choose Create B-L2 Access Interface. The B-L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- MC Ring Node
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to accept the fault propagation from the facility tunnel MEP.

7 Choose a transit prefix policy for the interface, if required.

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy - B-L2 Access Interface list form opens.

ii Select a transit prefix policy and click on the OK button.

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - B-L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - B-L2 Access Interface list form closes, and the B-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab button.

10 Click on the Select button to choose a port for the B-L2 access interface. The Select Terminating Port - VPLS B-L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS B-L2 Access Interface form closes, and the VPLS B-L2 Access Interface (Create) form displays the port information.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

For a B-L2 access interface, only Null, dot1q, and Q in Q encapsulation are supported.

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

13 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-B-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-B-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

14 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

15 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is dot1q or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - B-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you select an access ingress policy that has a forwarding class mapped to an ingress queue group, the port that you choose for the VPLS L2 access interface must use the same access ingress queue group.

See Procedure 20-1 for information about configuring Ethernet ports. See chapter 46 for information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - B-L2 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you select an access egress policy that has a forwarding class mapped to an egress queue group, the port that you choose for the VPLS L2 access interface must use the same access egress queue group.

See Procedure 20-1 for information about configuring Ethernet ports. See chapter 46 for information about queue group template policies.

vii If the port you selected in step 10 is not an HSMDA port then go to step 16.

viii Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

ix Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

x Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

xi Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xii Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

16 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 18.

Note — The Schedulers tab is configurable only when a port is assigned to the interface.

17 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 10 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 10 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - B-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS B-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 10 is an HSMDA port, go to step 18.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - B-L2 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS B-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 18.

b Specify that an access scheduler policy is applied to the interface.

Note — You cannot specify an access scheduler policy if the port you selected in step 10 is an HSMDA port. Go to step 18.

i Set the Aggregation parameter to on.

ii Configure the Frame-Based Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - B-L2 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

18 Assign ingress and egress ACL filters to the interface, if required.

Note — Only MAC filters are allowed for B-L2 Access Interfaces.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - B-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - B-L2 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

19 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - B-L2 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the accounting policy name.

20 Configure BPDU Termination, STP, FIB, and MRP parameters for the interface, if required.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination
  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface
  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS B-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step xiv.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The B-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the B-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the new MST instance.

xiii If you are configuring an MVPLS B-L2 access interface, go to step 21.

xiv Click on the MRP tab button.

xv Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave All Time (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

Note — You can view information regarding MMRP Entries by clicking on the MMRP tab button.

xvi Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

xvii Choose the desired policy and click OK.

21 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - B-L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - B-L2 Access Interface form closes and the policy ID is displayed on the B-L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

22 Configure a redundant VLAN range, if required.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Create button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

23 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

24 Specify the queue overrides.

i Click on the Override Policy Items tab button.

Note — The Override Policy Items tam contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

ii See Procedure 47-44 for information about setting queue overrides.

25 Associate a MEP with the B-L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Maintenance Entity Group list form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group list form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Interface Type

Note — The Interface Type parameter is automatically selected based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

vi Click on the Select button. The Select SAP - MEP form opens.

vii Select a SAP in the list and click on the OK button. The MEP form displays the SAP information.

viii If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step xii.

ix Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

x Click on the AIS tab button.

xi Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xii Click on the OK button. The MEP (Create) form closes.

26 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button. The ANCP Static Map (Create) form opens.

ii Configure the ANCP String parameter.

iii Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

- **iv** Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

- **v** Click on the OK button. The ANCP Static Map form closes.

27 Click on the OK button. The B-L2 Access Interface (Create) form closes and a dialog box appears.

28 Click on the OK button. The VPLS (Edit) form reappears.

29 Repeat steps 4 to 28 for each additional B-L2 access interface that you want to create.

30 Click on the OK button. A dialog box appears.

31 Click on the Yes button. The VPLS (Edit) form closes.

32 Close the Manage Services form.

Procedure 71-14 To create a VPLS I-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

5 Right-click on Access Interfaces and choose Create I-L2 Access Interface. The I-L2 Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Description
- Administrative State
- MC Ring Node
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept.

7 Choose a transit prefix policy for the interface, if required.

- **i** Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy - VPLS I-L2 Access Interface list form opens.

- **ii** Select a transit prefix policy and click on the OK button.

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - I-L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - I-L2 Access Interface list form closes, and the I-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab button.

10 Click on the Select button to choose a port for the I-L2 access interface. The Select Terminating Port - VPLS I-L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS I-L2 Access Interface form closes, and the VPLS I-L2 Access Interface (Create) form displays the port information.

Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

For an I-L2 access interface, only Null, dot1q, and Q in Q encapsulations are supported. In the case of I-MPVLS L2-access interfaces, Null encapsulation is not supported. I-MPVLS L2-access interfaces with MSTP configured support Q in Q. These ports must also be of Ethernet type PBB.

When the selected port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet with Q in Q encapsulation.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

13 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

14 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-I-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-I-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

15 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

16 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is dot1q or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - I-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - I-L2 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

vii If the port you selected in step 11 is not an HSMDA port then go to step 17.

viii Configure the Packet Byte Offset (bytes) parameter, if required. Before you can configure the parameter, you must select the associated Override check box.

ix Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

x Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the WRR policy information displayed.

xi Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xii Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

17 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 19.

Note — The Schedulers tab is configurable only when a port is assigned to the interface.

18 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 11 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 11 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - I-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS I-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 11 is an HSMDA port, go to step 19.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - I-L2 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPLS I-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 19.

b Specify that an access scheduler policy is applied to the interface.

Note — You cannot specify an access scheduler policy if the port you selected in step 11 is an HSMDA port. Go to step 19.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - I-L2 Access Interface form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

19 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - I-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

- **iv** Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - I-L2 Access Interface form opens.

- **v** Select an egress ACL filter and click on the OK button. The Select Egress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

- **vi** Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - I-L2 Access Interface form opens.

- **vii** Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

- **viii** Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - I-L2 Access Interface form opens.

- **ix** Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

20 Assign an accounting policy to the interface, if required.

- **i** Click on the Accounting tab button.

- **ii** Configure the Collect Accounting Statistics parameter.

- **iii** Click on the Select button to choose an accounting policy. The Select Accounting Policy - I-L2 Access Interface form opens.

- **iv** Select an accounting policy and click on the OK button. The Select Accounting Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the accounting policy name.

21 Configure BPDU Termination, STP, and FIB parameters for the interface, if required.

- **i** Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

- **ii** Configure the parameters:

  - L2 Protocol Termination
    When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
  - BPDU Translation
  - Force L2PT on Managed L2 Access Interface
    The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS I-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

- **iii** Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step 22.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The I-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the I-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the new MST instance.

22 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - I-L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - I-L2 Access Interface form closes and the policy ID is displayed on the I-L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

23 Configure an Ethernet tunnel.

Note — You can only configure Ethernet tunnel SAP path parameters if you are creating a same-fate SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 24.

iii Click on the Create button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

24 Configure a redundant VLAN range, if required.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Create button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

25 Configure IGMP snooping for the interface, if required.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast Leave
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Maximum Number of Sources per Group

The General Query Interval (seconds), Maximum Response Interval (seconds), Robust Count, and IGMP Version parameters are configurable when the Send Queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 26.

iv Click on the Create button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create additional entries. A dialog box appears.

vii Click on the OK button.

viii Repeat steps iv to vii to create an additional entry, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

26 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

27 Specify the queue overrides.

i Click on the Override Policy Items tab button.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

ii See Procedure 47-44 for information about setting queue overrides.

28 Associate a MEP with the I-L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Maintenance Entity Group list form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group list form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Interface Type

Note — The Interface Type parameter is automatically selected based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

vi Click on the Select button beside the Name parameter. The Select SAP - MEP form opens with a list of service access interfaces for the MEP.

vii Choose a service access interface from the list.

viii Click on the OK button. The MEP form is refreshed with the SAP information.

ix If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step xiii.

x Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xi Click on the AIS tab button.

xii Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xiii Click on the OK button. The MEP (Create) form closes.

29 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

30 Click on the OK button. The I-L2 Access Interface (Create) form closes and a dialog box appears.

31 Click on the OK button. The VPLS (Edit) form reappears.

32 Repeat steps 4 to 31 for each additional I-L2 access interface that you want to create.

33 Click on the OK button. A dialog box appears.

34 Click on the Yes button. The VPLS (Edit) form closes.

35 Close the Manage Services form.

Procedure 71-15 To configure a GNE site on a VPLS service

Use this procedure to add a GNE site and GNE service interfaces to an existing VPLS service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on VPLS Service and choose Create GNE Site. The Select Network Elements - VPLS Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab button and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab button and then click on the Select button next to the Interface Index field. The Select Generic NE Interface form appears.

iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encap Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab button to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The VPLS (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The VPLS (Edit) form closes.

You can use the topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 71-16 To force a switchover to a redundant spoke SDP binding

This procedure can only be performed on a VPLS that has been configured with endpoints that are associated redundant spoke SDP bindings.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site where you want to perform the switchover; expand the entries for that site.

5 Right-click on the redundant spoke SDP binding under an endpoint for the site that you want to perform the switchover for.

6 Select Force Switchover from the popup menu.

7 You can clear the switchover at a later time by performing steps 1 to 5 again and then select the Clear Forced Switchover item from the popup menu.

Note — You must clear a manually forced switchover by using the Clear Forced Switchover button when the active spoke SDP binding is restored. The 5620 SAM cannot automatically switch to another active spoke SDP binding if this is not done.

8 Click on the OK button to close the Spoke SDP Binding (Edit) form.

9 Click on the OK button to close the VPLS (Edit) form.

Procedure 71-17 To run a VPLS service OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 78 for more information about how to create a validator test suite.

Note — OAM validation tests are not supported for HVPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

  i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

  ii Configure the filter criteria. A list of OAM validator test suites appears.

  iii Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failed indicator.

6 Click on the Tests tab button. The Test Suite tab is displayed.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPLS (Edit) form.

15 Close the Manage Services form.

Procedure 71-18 To add or modify FIB entries associated with a VPLS

1 Choose Manage→Service→FIB Entries from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Control tab button.

5 Click on the FIB Entries tab button.

6 Click on the Find button. A list of FIB entries appears.

7 Add or modify FIB entries as required.

 a To add a FIB entry:

  i Click on the Create button. The FibEntry (Create) form opens.

  ii Configure the parameters:

   - MAC Address
   - Auto Complete

  iii Choose an interface, service circuit, or endpoint from the list on the L2 Interfaces, Service Circuits, or Endpoints tab.

  iv Click on the OK button. The FibEntry (Create) form closes, and the FIB Entries form refreshes with the new FIB entry.

 b To modify FIB entries:

  i Select a FIB entry on the FIB Entries tab and click on the Properties button. The FibEntry (Edit) form opens.

  ii Configure the parameters and view the information as required.

  iii Click on the OK button. A dialog box appears.

  iv Click on the OK button to close the VPLS (Edit) form.

Procedure 71-19 To list FIB entries associated with a VPLS

1 Choose Manage→Service→FIB Entries from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button.

5 Click on the VPLS, B-VPLS, or I-VPLS tab buttons, if required.

6 Select the site can click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

7 Click on the Forwarding Control tab button.

8 Click on the FIB Entries tab button.

9 Click on the Resync button for the FIB entries on the right side of the form. The Resync button on the bottom of the form is for re synchronizing the entire VPLS site.

10 Click on the Find button. A list of FIB entries appears.

Procedure 71-20 To view the service topology associated with a VPLS service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Topology View button. The Service Topology map opens.

See chapter 5 for more information about service topology views.

Note — In the VPLS topology map view, a redundant spoke SDP binding under an endpoint displays differing colors, depending on whether it is in the active or backup state. Backup spoke SDP bindings are shown in purple.

4 Close the Service Topology form.

5 Close the Manage Services form.

Procedure 71-21 To view the VPLS service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPLS (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object, if required.

8 Click on the Tests tab button if the OAM Validation Failed indicator is enabled. You can view the OAM validation test suite results by clicking on the Validation Result tab.

Note — You can run the OAM Validation test suite for this service from this form by clicking on the More Actions > Validate button.

9 Close the VPLS (Edit) form.

10 Close the Manage Services form.

Procedure 71-22 To view IGMP snooping queriers

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on a site. The Site (Edit) form opens with the General tab displayed.

5 Click on the IGMP Snooping tab button. The General tab is displayed.

6 Click on the MRouters tab button. The MRouters table displays a list of IGMP snooping queriers and their properties.

7 Click on the Refresh button to view periodic updates to the Mrouters table.

8 Close the Site (Edit) form.

9 Close the VPLS (Edit) form.

Procedure 71-23 To view MLD snooping queriers

1. Choose Manage→Service→Services from the 5620 SAM main menu.
2. Configure the filter criteria. A list of services appears.
3. Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.
4. On the navigation tree, click on a site. The Site (Edit) form opens with the General tab displayed.
5. Click on the MLD Snooping tab button. The General tab is displayed.
6. Click on the MRouters tab button. The MRouters table displays a list of MLD snooping queriers and their properties.
7. Click on the Refresh button to view periodic updates to the Mrouters table.
8. Close the Site (Edit) form.
9. Close the VPLS (Edit) form.

Procedure 71-24 To modify a VPLS

Caution — Modifying parameters can be service-affecting.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears.
3. Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

The following tabs contain parameter information for the service:

- General tab—displays the general service properties
- MVR tab—displays multicast package policy information for the service
- Tests tab—allows the creation and execution of service-specific diagnostic tests
- Forwarding Control tab—lists the FIB and STP instances
- Sites tab—lists the sites that belong to the service
- L2 Access Interfaces tab—lists the L2 access interfaces that belong to the service
- L2 Management Interfaces tab—lists the L2 management interfaces that belong to the service
- Mesh SDP Bindings tab—displays the mesh SDP bindings that belong to the service
- Spoke SDP Bindings tab—displays the spoke SDP bindings that belong to the service, including active and backup SDP bindings associated with endpoints.
- Endpoints tab—displays the endpoints associated with the service
- Template tab—displays the template used to create the service, if applicable
- Faults tab—displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Navigate to related components for the service using the navigation tree, as required.

Certain service components have related objects that can be easily examined using the navigation tree. For such objects, right-clicking them in the navigation tree offers a “Navigate to ...” option in the contextual menu. If you select this option, the properties form for the related object is displayed. This can be very convenient, especially for complex services containing many sites and components.

The VPLS components for which you can navigate to such related objects include:

- I-Sites: you can navigate to the associated B-VPLS or B-(M)VPLS
- L2 Access Interfaces: you can navigate to the opposite SAP in a VLAN Uplink configuration
- Redundant L2 Access Interfaces: you can navigate to the opposite SAP.
- Mesh SDP Bindings: you can navigate to the opposite (return) mesh SDP
- Spoke SDP Bindings: you can navigate to the opposite (return) spoke SDP

5 Modify the components and parameters for the service, as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The VPLS (Edit) form closes, and the Manage Services form reappears.

8 Close the Manage Services form.

Procedure 71-25 To modify a VLPS using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 10.
- Creating SDP bindings. Go to step 23.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS Site
- VPLS B-Site
- VPLS I-Site

5 Select the required option. The Select Network Elements form appears.

6 Select one or more sites to add to the service and click OK. The VPLS Site (Create), VPLS I-Site (Create), or VPLS B-Site (Create) form is displayed, depending on your menu item selection. If you selected more than one site, the VPLS Site (Multiple Instances) (Create), VPLS I-Site (Multiple Instances) (Create), or VPLS B-Site (Multiple Instances) (Create) form is displayed, depending on your menu item selection.

7 Click on OK. The VPLS Site (Create) (or VPLS Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

8 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The VPLS Site (Edit) form opens. Refer to Procedure 71-1 for detailed site configuration information.

9 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating site components

10 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS L2 Access Interface (this choice will actually display as either a regular L2 Access Interface, or a B-L2 or I-L2 variant, depending on the site you select). Go to step 11.
- VPLS L2 Management Interface. Go to step 15.
- VPLS Endpoint. Go to step 19.

11 If you choose to create a VPLS L2 Access Interface, then the VPLS L2 Access Interface (Create) form is displayed. If the selected site is a B-Site or I-Site, then the B-L2 or I-L2 Access Interface (Create) form is displayed accordingly.

12 Click on the Port tab and assign a port to the interface.

Refer to Procedure 71-3 (or Procedure 71-13 or 71-14 for B-L2 or I-L2 Access Interfaces respectively) for detailed information on further configuring the interface, if required.

13 Click OK. The VPLS L2 Access Interface (Create) form closes.

14 Go to step 22.

15 If you choose to create a VPLS L2 Management Interface, then the VPLS L2 Management Interface (Create) form is displayed.

16 Click on the Port tab and assign a port to the interface.

Refer to Procedure 71-3 for detailed information on further configuring the interface, if required.

17 Click OK. The VPLS L2 Management Interface (Create) form closes.

18 Go to step 22.

19 If you choose to create a VPLS Endpoint, then the Endpoint (Create) form is displayed.

20 Configure the Name parameter for the endpoint.

Refer to Procedure 71-1 (or 71-11 for B-Sites) for detailed information on further configuring the endpoint, if required.

21 Click OK. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

22 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating SDP bindings

23 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note 1 — If you intend to create either a spoke or a mesh binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

Note 2 — If you intend to create a full mesh between sites, then the order in which you select the sites is not important.

Note 3 — If you intend to add a service site to an existing mesh of sites, then the first site you select must be the one that is not currently a part of the mesh. The second site you select can be any member of the existing mesh.

24 Select Connect from the contextual menu. Depending on the sites you selected, one or more of the following options are available:

- Create Spoke SDP Binding. Go to Step 25.
- Create Mesh SDP Binding. Go to Step 32.
- Create Full Mesh. Go to Step 39.
- Add To Existing Mesh. Go to Step 46.

25 If you choose the Create Spoke SDP Binding option, then the Spoke SDP Binding (Create) form is displayed.

Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

26 Enable the Auto-Select Transport Tunnel parameter.

27 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 71-5 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

28 Assuming that the spoke SDP binding was successfully created in step 27, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

29 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

30 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

31 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

32 If you choose the Create Mesh SDP Binding option, then the Mesh SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

33 Enable the Auto-Select Transport Tunnel parameter.

34 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 71-4 for more detailed information on creating and configuring mesh bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

35 Assuming that the mesh SDP binding was successfully created in step 34, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a mesh binding for the return tunnel.

36 Right-click on the second site you selected and choose the Create Mesh SDP Binding ... option from the contextual menu. The Mesh SDP Binding (Create) form is displayed.

37 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

38 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

39 If you choose the Create Full Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

40 Configure the Transport Type parameter.

41 Click the Select button to display the Tunnel Selection Profiles form, if required.

42 Click Search to display a list of available Tunnel Selection Profiles.

43 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

44 Click OK to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 71-4 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between all the sites, then the new bindings that can be created are displayed, and an error message is also displayed informing you that the full mesh could not be completed. Refer to Chapter 33 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

46 If you choose the Add To Existing Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

47 Configure the Transport Type parameter.

48 Click the Select button to display the Tunnel Selection Profiles form, if required.

49 Click Search to display a list of available Tunnel Selection Profiles.

50 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

51 Click OK to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 71-4 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between the selected sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

52 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

53 Close the Service Topology form.

54 Close the Manage Services form.

Procedure 71-26 To delete a VPLS

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

Note — A VPLS cannot be deleted if the L2 access interface has MSAPs that are in an active state. See chapter 68 for more information about MSAPs.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services, regardless of the priority configuration, acknowledge the check box that prompts you to confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

72 — Mirror service management

72.1 Mirror service overview

The 5620 SAM GUI implementation of service mirroring provides mirroring of service traffic packets from any service type.

Caution — Service mirroring can affect performance across the network and in the source and destination devices, so must be planned accordingly.

In a mirror service, packets from one or more sources are forwarded to their normal destinations and a copy of the entire packet, or a specified portion of the packet, is sent to the mirror destination. The mirrored packet can be viewed using a packet-decoding device, typically called a sniffer, that is attached to the destination port. The 5620 SAM does not limit the number of destination and source sites added under a mirror service. The mirrored packets are transported unidirectionally through the core network using IP or MPLS tunneling.

With pseudo-wire redundancy support, an ICB can be enabled in the mirror service spoke and remote source, which can provide bidirectional service that enables support for active and standby PE redundancy. An endpoint can be used to group the redundant objects, which may be of mirror SDP bindings or SDP and SAP. In the mirror map view, the color for the active and backup states of the redundant mirror SDP differ.

Service mirroring can be used to do the following:

- Troubleshoot problems with customer packet delivery and content.
- Help service providers meet regulations by providing itemized call records and wiretaps, as authorized by investigative authorities.
- Simplify the complex traffic-analysis networks that are often implemented as overlays to the customer-facing network.

The 5620 SAM supports end-to-end mirror service configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the admin role, or mirror service management with the template management role can create a mirror service template.
- A separate lawful intercept management scope of command role allows a LI user to view and configure LI sources on existing mirror services. Information that is mirrored is hidden from all users who do not have LI user privileges. See chapter 34 for more information about configuring a LI user.

The mirror service operational status is aggregated based on the status of each site.

- Aggregate status is down if all destination sites are down.
- Aggregate status is up if one of the redundant destination site is up.
- Aggregate status is down if all source sites are down.
- Aggregate status is up if one of the redundant source sites is up.
- Aggregate status is unknown if no sites are added to the service.

Consider the following information before you implement a mirror service:

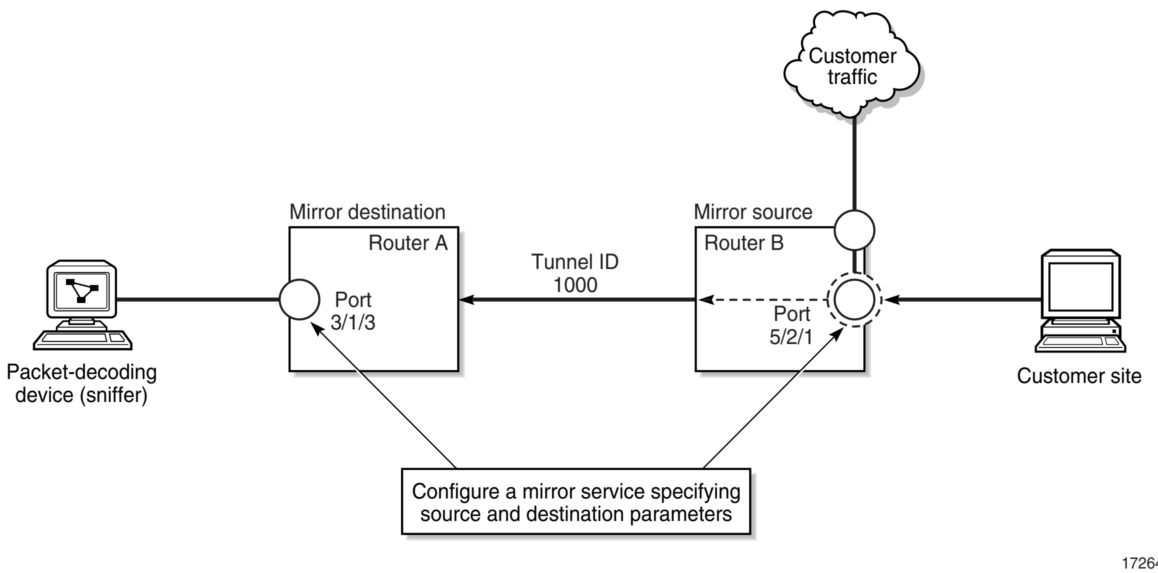
- The default customer is automatically associated with a mirror service. You cannot associate a different customer with a mirror service.
- You can configure one endpoint per mirror site.
- You can configure the endpoint in the destination site with SAP and SDP with ICB.
- An endpoint cannot have more than one SAP.
- You can create a mirror SDP under the endpoint in the destination site.
- You can create up to four mirror SDPs under the endpoint in the source site. One mirror SDP must have ICB. Another option is to create one mirror SDP under the source site.
- When the mirror SDP binding is under an endpoint, the STP cannot be enabled on the spoke.
- Mirror sites with valid SAP are considered as destination sites during discovery.
- You can configure site as destination without SAP in the mirror service. During re-synchronization, site type will be kept as destination.
- Auto-SDP creation is restricted to one destination.
- You can change the redundancy setting of a mirror SDP binding by deleting and adding the mirror SDP binding on an endpoint.
- You cannot delete an MC-LAG SAP if an ICB is on the same endpoint.
- You cannot have a SAP with non-ICB mirror spoke on the same endpoint.
- The destination of a mirror service must be an L2 SAP.
- You must be assigned the administrator or mirror service management scope of command role to create or modify a mirror service, or to view any mirror-related objects in the 5620 SAM.
- You can mirror the ingress or egress traffic on SAPs and ports.
- You can mirror the ingress or egress traffic that is associated with one or more subscriber hosts.
- You can specify match criteria, such as IP addresses, MAC addresses, or MPLS ingress labels, to filter the mirrored traffic.
- Mirror service IDs are obtained from the same pool of IDs that is used by other services. When you manually assign an ID value, ensure that you do not assign an ID that belongs to another service.
- Use the packet-slicing option to copy a specific packet size from each frame. This option is useful for monitoring network usage without copying the customer data. It also limits the amount of mirrored traffic that travels through the core network.
- When the mirror destination is not on the same NE as the mirror source, a mirror service requires a service tunnel between the source and destination NEs.
- The 5620 SAM can automatically create a service tunnel between the source and destination sites when the following conditions are met:
  - Automatic mesh SDP binding creation is enabled.
  - GRE or LDP is the transport type.
  - No other service tunnel is available between the source and destination sites.
- The mirror service source and destination encapsulation types must be the same.

- After an NE reboot or CPM activity switch, the debug configuration file for a mirror service is not by default reloaded on the NE. The 5620 SAM raises an alarm when this occurs. To ensure that the NE reloads the debug configuration file, you must specify the location of the file in the base 5620 SAM configuration. See chapter 6 for more information.
- When multiple mirror services reference the same packet, for example, from a SAP and from a port, the packet is mirrored only once, based on the following criteria in the following non-configurable order:
  - MAC or IP filters
  - MPLS ingress label
  - SAP
  - port
- For IP-only mirroring:
  - Requires chassis mode C or D to be enabled.
  - By using “IP Only” as the encapsulation type, users can specify that only the IP packet is mirrored, without its original ATM/FR/POS/Ethernet DLC header.
  - When IP-only is configured on the source site, users can configure various mirroring sources, including subscribers and SAPs from Ipipe, IES, VPRN, VPLS, and MVPLS services. However, source ports and VLL services including Apipe, Epipe, and Fpipe cannot be configured.
  - For local IP-only mirroring, the source and destination MAC addresses must be configured.
  - For remote IP-only mirroring in a VPRN service, an IP mirror interface on the VPRN destination node is used to receive the IP mirror packets and route them to the appropriate sniffer. If there are multiple sniffers connected to the VPRN using L3 interfaces, users need to configure the routing policy to have IP mirror packets routed to the correct sniffer.
- For LI source configuration:
  - You must be assigned the lawful intercept management scope of command role to view, create or modify any LI-related objects in the 5620 SAM.
  - LI source configurations are saved on an NE when the poller policy for the NE specifies LI Local Save Allowed. See chapter 13 for information about configuring in-band and out-of-band polling policies.

72.2 Sample mirror service configuration

Figure 72-1 shows a sample mirror service configuration.

Figure 72-1 Sample mirror service configuration



In this sample, Router B is the mirror source that carries the customer packets. Router A is the mirror destination. The ingress and egress traffic on Port 5/2/1 is mirrored on the destination, Port 3/1/3. Table 72-1 lists the high-level tasks to configure the sample mirror service.

Table 72-1 Sample mirror service configuration

Task	Description
1. Connect the packet sniffer to the mirror destination.	The packet sniffer is attached to Router A, Port 3/1/3.
2. Configure the mirror destination parameters.	Port 3/1/3 on Router A is specified as the mirror destination. Specify the Tunnel ID 1000 as the transport tunnel to the mirror destination. All the parameters required to configure the type of mirroring, for example, slicing and mirror classification, are specified in the destination parameters.
3. Specify the source entity that is to be mirrored.	The egress and ingress traffic on Port 5/2/1 is to be mirrored.

72.3 Workflow to create a mirror service

The following workflow lists the high-level steps required to create a mirror service. As a prerequisite for creating a mirror service, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1.

- the access ports for the service are created; see chapter 20 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.
- the network services the mirror service will use are created.
- a packet-sniffing device at the L2 SAP that is the destination of the mirror service is configured.
- the SAP with the attached packet-sniffing device as the mirror destination is specified.
- the source of the packets to be mirrored is configured.

1 Create the mirror service. See Procedure 72-1.

i Define the general properties for the mirror service.

ii Specify the services for inclusion in the mirror service. You can specify multiple services in one operation.

iii Enable one or more routing protocols for the mirror site.

iv Specify an endpoint on the site as a mirror source.

v Specify one or more SAPs on the site as a mirror source.

vi Specify one or more ports on the site as a mirror source.

vii Specify one or more IP filters for the source site.

viii Specify one or more MAC filters for the source site.

ix Specify one or more MPLS ingress labels for the source site.

x Specify one or more subscribers or subscriber hosts as mirror sources

xi Turn up the mirror service.

2 As required, view mirror service information:

a View the service topology map associated with a Mirror Service. See Procedure 72-2.

b View the mirror service operational status. See Procedure 72-3.

c To view LI mirrored subscriber hosts configured with a RADIUS server. See Procedure 72-4.

3 As required, run an OAM validation test for a mirror service. See Procedure 72-5.

4 As required, modify a mirror service. See Procedure 72-6.

5 As required, delete a mirror service. See Procedure 72-7.

72.4 Mirror service procedures

Use the following procedures to create, delete, view, and modify mirror services.

Procedure 72-1 To create a mirror service

1 Choose Create→Service→Mirror from the 5620 SAM main menu. The Mirror Service (Create) form opens with the General tab displayed.

2 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Priority
- Administrative State
- Automatic SDP Binding Creation
- OLC State
  This parameter is configurable when you click on the Apply button.

3 Perform one of the following:

a Leave the Automatic SDP Binding Creation parameter disabled.

When you leave the Automatic SDP Binding Creation parameter disabled, you must create SDP bindings for the service and bind the SDPs to a service tunnel in step 45 of this procedure.

b Enable the Automatic SDP Binding Creation parameter.

When you enable the Automatic SDP Binding Creation parameter, SDP bindings for the service are automatically created and bound to service tunnels.

i Configure the Transport Type parameter.

Note 1 — You must select GRE or LDP as the transport type to allow the 5620 SAM to automatically create SDP bindings between the source and destination sites. Automatic creation of SDP bindings cannot be configured if a service tunnel already exists between the source and destination sites.

Note 2 — To use MPLS:RSVP as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See chapter 33 for more information.

ii Configure the Use Bandwidth-Reserved Paths parameter, if applicable.

The Use Bandwidth-Reserved Paths parameter is configurable only when the Transport Type parameter is set to MPLS:RSVP or Any.

4 On the navigation tree, right-click on Destination Site and choose Create Destination Site from the contextual menu. The Select Network Elements - Mirror Service form opens with a list of available sites displayed.

5 Select a site and click on the OK button. The Select Network Elements - Mirror Service form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed in the Network Element panel.

6 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Encapsulation Type

7 Click on the Mirroring Configuration tab button.

8 Configure the parameters.

- Source Administrative State
- Slice Size
- Forwarding Class
- Enable Port ID Mirroring

Choose the default of 0 for the Slice Size parameter when you configure a destination mirror site, unless slicing at the destination is necessary. Packet slicing reduces the amount of mirrored traffic that traverses the network.

Note — The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only.

The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. If a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites.

9 Click on the Source Far Ends tab button.

10 Click on the Create button. The Remote Source (Create) form appears.

11 Configure the parameters.

- Remote Site ID
- Ingress Label
- Remote VC ID
- Remote ICB

12 Click on the OK button. The Remote Source (Create) form closes and a dialog box appears.

13 Click on the OK button. The Mirror Site (Create) form displays the remote source information.

14 Click on the OK button. The Site (Create) form closes and a dialog box appears.

15 Click on the OK button. The Mirror Service (Edit) form reappears with the service navigation tree displayed.

16 Expand the Destination Site object to reveal the newly created site.

17 Expand the newly created destination site object.

18 Configure an L2 access interface as the mirror destination by selecting L2 Access Interface (Test Equipment Interface) under the destination site in the service navigation tree, right-clicking on it and choosing Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

19 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

20 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

21 Configure the parameters.

- Outer Encapsulation Value
- Auto-Assign ID
- Inner Encapsulation Value

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

22 Assign an egress QoS policy to the interface, if required.

i Click on the QoS tab button.

ii Configure the Egress Mark QinQ Top Bits Only parameter.

iii Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

iv Configure the filter criteria. A list of egress policies appear at the bottom of the Select Egress Policy - L2 Access Interface form.

v Select an egress policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form refreshes with the egress QoS policy information displayed.

23 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L2 Access Interface form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface form closes and the L2 Access Interface (Create) form refreshes with the time of day suite information displayed.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Mirror (Create) form refreshes with the L2 access interface information displayed below L2 Access Interface (Test Equipment Interface) in the service navigation tree.

24 Click on the Schedulers tab button, if required.

25 Configure the Aggregate Rate Limit (kbps) parameter.

26 Click on the IP Mirror MAC Addresses tab, if you are configuring local mirroring and you chose IP Only as the encapsulation type in step 6. Otherwise, go to step 28.

Note — If you want to configure remote mirroring in a VPRN service, you must create an IP Mirror Interface in that service. See chapter 74 for more information.

27 Configure the parameters:

- Destination MAC Address
- Source MAC Address

Note — The Source and Destination MAC addresses on L2 Access Interface must be both null or neither null. Both null means that there are no source or destination MAC addresses configured on the interface.

28 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

29 Create an endpoint on the mirror site for redundancy support, if required.

i On the navigation tree, right-click on the Endpoints object below the site and choose Create Endpoints. The Endpoint (Create) form opens.

ii Configure the parameters.

- Name
- Description
- Revert Time (seconds)
- Disable Revert Time

iii Click on the Ok button.

For the destination site, the L2 Access Interface (Test Equipment Interface) and Mirror SDP Binding objects appear under the Endpoints object.

For the source site, the Mirror SDP Binding object now appears under the Endpoints object.

iv To create an L2 access interface as the mirror destination, right-click on the L2 Access Interface (Test Equipment Interface) object under the Endpoints object and choose Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

v Click on the Port tab button.

vi Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

vii Use the configurable filter and Search button to choose a port, and click on the Search button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

viii Configure other parameters, as required.

ix Click on the OK button on the L2 Access Interface (Create) form. The form closes and a dialog box appears.

x Click on the OK button. The SAP object appears under the L2 Access Interface object.

xi To create a mirror SDP binding on the endpoint, right-click on the Mirror SDP Binding object under the Endpoints object in the service navigation tree and choose Create Mirror SDP Binding from the contextual menu. The Mirror SDP Binding (Create) form opens.

xii Configure the parameters.

- Tunnel Termination Site
- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

xiii Click on the OK button. The Mirror SDP Binding (Create) form closes and a dialog box appears.

xiv Click on the OK button. The Mirror Service (Edit) form reappears with the service navigation tree displayed.

30 A mirror source can be on the same site as the mirror destination. If no mirror sources are on the destination site, go to step 37.

31 Specify a SAP on the site as a mirror source, if required. Perform one of the following:

a Right-click on the Source SAPs object below the site in the service navigation tree and choose Create Source Interface from the contextual menu. The Source Interface (Create) form opens. Go to step i.

b Right-click on the LI Source SAPs object below the site in the service navigation tree and choose Create LI Source Interface from the contextual menu. The LI Source Interface (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose an access interface to associate with the source interface. The Select Mirrored Interface - Source Interface form opens.

ii Use the configurable filter and Search button to choose an access interface, and click on the OK button. The Select Mirrored Interface - Source Interface form closes and the Source Interface (Create) form refreshes with the selected interface information displayed.

iii Configure the parameters.

- Enable Egress
- Enable Ingress

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Mirror Service (Create) form refreshes with the source SAP displayed below Source SAPs in the service navigation tree.

vi Repeat steps i to v to specify an additional source SAP for the site.

32 Specify a port on the site as a mirror source, if required.

i Right-click on the Source Ports object below the site in the service navigation tree and choose Create Source Port from the contextual menu. the Source Port (Create) form opens

ii Click on the Select button to choose a port. The Select - Source Port form opens.

A source port can be one of the following:

- physical port
- channel
- LAG
- bundle
- CCAG

iii Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Source Port form closes and the Source Port (Create) form displays the port information.

iv Configure the parameters.

- Enable Egress
- Enable Ingress

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Mirror Service (Create) form refreshes with the source port displayed below Source Ports in the service navigation tree.

vii Repeat steps i to v to specify an additional source port for the site.

33 Specify an IP filter entry for the mirror source, if required. Perform one of the following:

a Right-click on the Source IP Filters object below the site in the service navigation tree and choose Create Source IP Filter from the contextual menu. The Source IP Filter (Create) form opens. Go to step i.

b Right-click on the LI Source IP Filters object below the site in the service navigation tree and choose Create LI Source IP Filter from the contextual menu. The LI Source IP Filter (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose an IP filter entry. The Select Filter - Source IP Filter form opens.

ii Use the configurable filter and Search button to choose an IP filter entry, and click on the OK button. The Select Filter - Source IP Filter form closes and the Source IP Filter (Create) form refreshes with the selected IP filter ID and IP filter entry ID displayed.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the source IP filter displayed below Source IP Filters in the service navigation tree.

v Repeat steps i to iv to specify an additional source IP filter.

34 Specify a MAC filter entry for the mirror site, if required. Perform one of the following:

a Right-click on the Source MAC Filters object below the site in the service navigation tree and choose Create Source MAC Filter from the contextual menu. The Source MAC Filter (Create) form opens. Go to step i.

b Right-click on the LI Source MAC Filters object below the site in the service navigation tree and choose Create LI Source MAC Filter from the contextual menu. The LI Source MAC Filter (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose a MAC filter entry. The Select Filter - Source Mac Filter form opens.

ii Use the configurable filter and Search button to choose a MAC filter entry, and click on the OK button. The Select Filter - Source Mac Filter form closes and the Source MAC Filter (Create) form refreshes with the selected MAC filter ID and MAC filter entry ID displayed.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the source MAC filter displayed below Source MAC Filters in the service navigation tree.

v Repeat steps i to iv to specify an additional source MAC filter.

35 Specify an MPLS ingress label for the mirror, if required.

i Right-click on the Source MPLS Ingress Labels object below the site in the service navigation tree and choose Create Source Ingress Label from the contextual menu. The Source Ingress Label (Create) form opens.

ii Configure the Ingress Label parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the MPLS ingress label displayed below Source MPLS Ingress Labels in the service navigation tree.

v Repeat steps i to iv to specify an additional source MPLS ingress label.

36 Specify a subscriber as a mirror source, if required. Perform one of the following:

a Right-click on the Source Subscribers object below the site in the service navigation tree and choose Create Source Subscriber from the contextual menu. The Source Subscriber (Create) form opens. Go to step i.

b Right-click on the LI Source Subscribers object below the site in the service navigation tree and choose Create LI Source Subscriber from the contextual menu. The LI Source Subscriber (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Configure the following parameters:

- Subscriber Identification String
- Forwarding Classes
- Enable Egress
- Enable Ingress

ii You can further restrict the mirrored subscriber host traffic associated with the subscriber identification string by specifying SAP or SLA-profile criteria. To specify an SLA profile as a match criterion, go to step viii.

Note — You can configure parameters in the SAP/Subscriber Host Match Criteria panel or the SLA Profile Match Criteria panel, but you cannot configure parameters in both panels.

iii Click on the Select button in the SAP/Subscriber Host Match Criteria panel to specify a SAP on which to mirror subscriber host traffic. The Select SAP ID/Encap Value - Source Subscriber form opens.

iv Configure the filter criteria and click on the Select button. A list of SAPs is displayed.

Note — The form lists only dot1q- or Q in Q-encapsulated SAPs that have subscriber management enabled.

v Select a SAP in the list and click on the OK button. The Select SAP ID/Encap Value - Source Subscriber form closes and the SAP information is displayed on the Source Subscriber (Create) form.

vi Configure the parameters in the SAP/Subscriber Host Match Criteria panel to specify the subscriber host match criteria for the SAP:

- Host IP Address
- Host MAC Address

Note — The 5620 SAM does not accept the parameter values unless a SAP is specified in step v.

vii Go to step x.

viii Click on the Select button in the SLA Profile Match Criteria panel. The SLA Profile - Source Subscriber form opens.

ix Select an SLA profile in the list and click on the OK button. The Select SLA Profile - Source Subscriber form closes and the SLA profile name is displayed on the Source Subscriber (Create) form.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Mirror Service (Create) form refreshes with the source subscriber listed below Source Subscribers in the service navigation tree.

xii Repeat steps viii to xi to specify an additional source subscriber, if required.

37 To configure a mirror source on a site other than the destination site, right-click on Source Sites in the service navigation tree and choose Create Source Site from the contextual menu. Otherwise, go to step 59.

38 The Select Network Elements - Mirror form opens with a list of available sites displayed. Select a site and click on the OK button. The Select Network Elements - Mirror form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed.

39 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Encapsulation Type

40 Click on the Mirroring Configuration tab button.

41 Configure the parameters.

- Source Administrative State
- Slice Size
- Forwarding Class
- Enable Port ID Mirroring

Note — The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only.

The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. On the other hand, if a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites.

42 Click on the OK button. A dialog box appears.

43 Click on the OK button. The Mirror Site (Create) form closes, and the Mirror Service (Create) form reappears with the selected site displayed on the navigation tree under Source Sites.

44 Expand the newly created site object.

45 Perform one of the following:

a If the Automatic SDP Binding Creation parameter was disabled in step 3, choose an SDP binding for the mirror source by selecting Mirror SDP Binding under the source site in the service navigation tree and then right-clicking and choosing Create Mirror SDP Binding from the contextual menu.

b Go to step 51.

46 The Mirror SDP Binding (Create) form opens. Specify a destination node for the mesh SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter to choose a destination for the SDP binding. The Select Destination Network Element - Mirror SDP Binding form opens.

ii Select a node and click on the OK button. The Select Destination Network Element - Mirror SDP Binding form closes and the Mirror SDP Binding (Create) form refreshes with the destination node ID displayed in the Tunnel Termination Site panel.

b If the destination node is not managed by the 5620 SAM, specify the system ID of the destination node for the Tunnel Termination Site parameter.

47 Configure the parameters.

- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

48 Perform one of the following to specify a transport tunnel for the mirror SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mirror SDP Binding form opens.

ii Select a service tunnel for the mirror SDP binding and click on the OK button. The Select Tunnel - Mirror SDP Binding form closes, and the Mirror SDP Binding (Create) form refreshes with the service tunnel identifier.

49 Click on the OK button. A dialog box appears.

50 Click on the OK button. The Mirror SDP Binding (Create) form closes and the Mirror (Create) form refreshes with the mirror SDP binding displayed under Mirror SDP Binding for the site.

51 To specify an endpoint on the site as a mirror source, perform step 29.

52 To specify one or more SAPs on the site as mirror sources, perform step 31.

53 To specify one or more ports on the site as mirror sources, perform step 32.

54 To specify one or more IP filters for the source site, perform step 33.

55 To specify one or more MAC filters for the source site, perform step 34.

56 To specify one or more MPLS ingress labels for the source site, perform step 35.

57 To specify one or more subscribers or subscriber hosts as mirror sources, perform step 36.

58 Perform one of the following:

a Configure an additional source site for the mirror service. Perform steps 37 to 56.

b Complete the mirror service configuration. Go to step 59.

59 Click on the OK button. A dialog box appears.

60 Click on the Yes button. The Mirror Service (Create) form closes.

Procedure 72-2 To view the service topology associated with a mirror service

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 5 for more information about service topology views.

Procedure 72-3 To view the mirror service operational status

The Aggregated Service Site Operational State and State Cause indicators on the General tab of the mirror service management form display information about service faults.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The alarms are grouped into various categories.

7 Close the Mirror Service (Edit) form.

8 Close the Manage Mirror Services form.

Procedure 72-4 To view LI mirrored subscriber hosts configured with a RADIUS server

Note 1 — You must have 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 34-6.

Note 4 — Only PPPoE subscriber hosts can be mirrored with RADIUS.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of mirror services appears.

3 Choose a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button. A list of mirror service sites are displayed.

5 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

6 If an LI source configuration object has not been created, the LI Source Configuration tab button is dimmed. Click on the Create LI Source Configuration button at the bottom of the form. A dialog box appears.

Note 1 — You must create an LI source configuration object for the NE to mirror subscriber hosts for LI.

Note 2 — The Create LI Source Configuration button is a toggle that also lets you delete an LI source configuration object. If you delete an LI source configuration object, all associated LI source objects are deleted.

Note 3 — An LI source configuration object is automatically created when an LI source object is created.

7 Click on the OK button. The LI Source Configuration tab button is enabled, and an LI source configuration object is created.

8 Click on the LI Source Subscribers Via RADIUS tab button.

9 Configure the filter criteria, if required, and click on the Search button. A dialog box appears.

10 Click on the OK button. A list of subscribers appears.

11 Choose a subscriber and click on the Properties button. The LI Source Subscriber Host form opens.

12 View the information on the form.

13 Close the LI Source Subscriber Host form.

Procedure 72-5 To run an OAM validation test for a mirror service

An OAM validator test suite must be created for the tested entity. See chapter 78 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Mirror Services form.

3 Select a service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

- **i** Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.
- **ii** Configure the filter criteria. A list of OAM validator test suites appears.
- **iii** Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the Mirror Service (Edit) form.

11 Close the Manage Mirror Services form.

Procedure 72-6 To modify a mirror service

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the other tab buttons to edit additional properties, as required.

5 Modify the parameters on the appropriate tab, as required.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The Mirror *Service Name* (Edit) form closes and the Manage Mirror Services form reappears.

8 Click on the Close button to close the Manage Mirror Services form.

Procedure 72-7 To delete a mirror service

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

73 — IES management

73.1 IES management overview

An IES is a routed connectivity service in which the customer traffic passes through an L3 IP router interface to the Internet.

IES allows customer-facing IP interfaces in the same routing instance to be used for service network core-routing connectivity. IES requires that the IP addressing scheme that is used by the customer be unique among other provider addressing schemes and potentially the entire Internet.

Packets that arrive at the edge device are associated with an IES based on the access interface on which they arrive. An access interface is uniquely identified using:

- port
- service ID
- IP address

IES configuration

The 5620 SAM supports end-to-end IES configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in IES of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 68 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 256 subnets. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays IES subscriber interfaces, group interfaces, and the associated SAPs.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT implementation in an IES requires a NAT configuration on the NE base routing instance and a NAT policy that is associated with a subscriber profile. See chapter 30 for information about configuring and deploying NAT on a base routing instance. See chapter 46 for information about configuring a NAT policy. See chapter 68 for information about associating a NAT policy with a subscriber profile.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 76 for more information about the hierarchical organization of composite services.

Common to all device services, such as IES, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy form.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 46 for more information about policies.

Although IES is part of the routing domain, the usable IP address space may be limited. IES allows a portion of the service provider address space to be reserved for service IP provisioning and to be administered by a separate, but subordinate, address authority.

Multiple IESs can be created to separate customer-owned IP interfaces. More than one IES can be created for one customer. More than one IP interface can be created in one IES. All IP interfaces created in an IES belong to the same customer.

The IES IP interfaces are restricted to the routing protocols that can be defined on the interface based on the fact that the customer has a different routing domain for this service. The IP interfaces support the following routing protocols:

- RIP
- OSPF

- BGP
- IS-IS
- PIM
- IGMP

Customer routes can be advertised to the network core using static routes, RIP, or BGP. BGP and static routes are the most commonly used routing methods.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

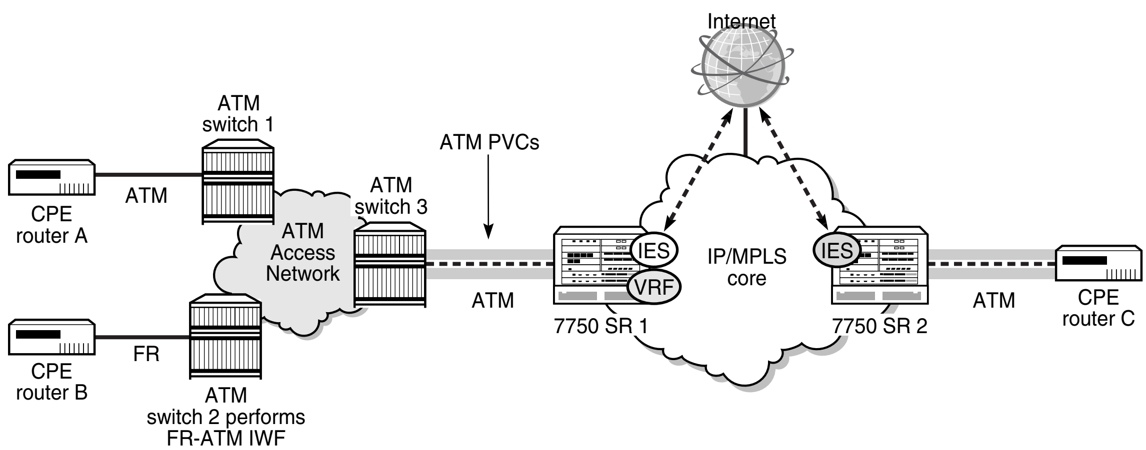
An IES can be connected to a VLL service or to a VPLS by an internal cross-connect through a CCAG adapter. This configuration eliminates the need for the physical port, cable, and other MDA-specific components and results in a less costly and more reliable interconnection. See chapter 76 for information about joining services to form composite services.

ATM SAP terminations for IES

CE routers that have access to an ATM network can connect with an IES service using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, and directly through ATM connections.

Figure 73-1 shows how CPE router A in an existing ATM network can access L3 IP services, such as an IES, using a statically configured ATM PVC on a 7750 SR (SR #1). CPE router B is connected to a Frame Relay, which connects to ATM switch 2 through IWF (service interworking). The RFC 2684-encapsulated traffic moves from both CPE routers through the ATM access network to a SAP configured on a 7750 SR #1 to serve a specific IES. At the same time, SDPs on the router are configured to a service to forward traffic over the IP/MPLS core. Destination CPE router C can receive RFC 2684-encapsulated traffic over an IP network over an ATM switch connected directly using 7750 SR #2.

Figure 73-1 ATM SAP network connection to an IES

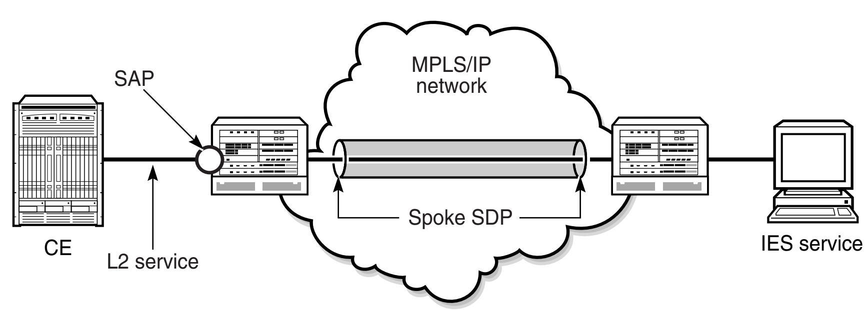


The two connection methods used between an ATM network and the IES router: LLC/SNAP encapsulation and VC multiplexing.

A VLL Epipe service can terminate directly on an IES service using an SDP spoke on the 7750 SR or 7450 ESS. Traffic that terminates on an IES service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by IES are also supported for spoke SDP termination.

Figure 73-2 shows a spoke SDP terminating directly on an IES. The spoke SDP could be tied to VLL Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 73-2 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID, which must be unique within the NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for each SRRP instance associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism that controls state transitions is based on a dynamic priority level that an SRRP instance maintains. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

To prevent a flood of AccessInterfaceDown alarms that an SRRP fault or link failure may generate for LAG-based MSAPs, the 5620 SAM performs alarm suppression. See chapter 68 for more information.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

The 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12 support DoS protection policies.

To protect an IES from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the IES L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on an IES L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each IES L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 21-3 for information about creating a DoS protection policy.

Local DHCP servers

The 5620 SAM supports configuring local DHCP servers on the 7710 SR, 7750 SR, and the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the Local DHCP server.

- Subscriber aggregation in a single node or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

Local user database

The 5620 SAM supports the configuration of a local user database on the 7450 ESS, 7750 SR, and 7710 SR. A local database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured or it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. After a local user database is configured, it can be associated with a local DHCP server and PPPoE configurations on group interfaces.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address are not authenticated.

PPPoE protocol on IES

An IES can be configured to support PPPoE. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used by DSL sessions with Ethernet framing to support multiple subscribers in a LAN. Using the group interface configuration form, you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

L2TP configuration for IES

An IES group interface can be configured to terminate LNS PPP sessions. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

After a tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

Note — If the LAC NE is a Release 7.0 7750 SR, each L2TP tunnel must have the local IP address set to the system interface IP address.

See chapter 18 for more information about ISA-LNS groups. See Procedure 18-7 for information about creating and configuring an ISA-LNS group. See chapter 31 for more information about L2TP. See Procedure 73-8 for information about configuring an IES group interface to terminate LNS PPP sessions.

73.2 Sample IES configuration

Figure 73-3 shows a sample IES configuration.

Figure 73-3 Sample IES configuration

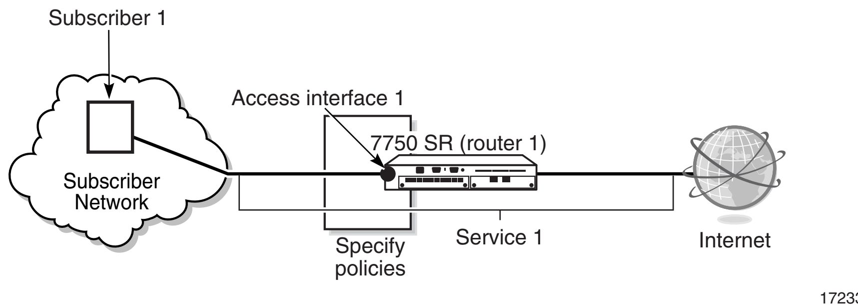


Table 73-1 lists the high-level tasks necessary to configure this sample IES.

Table 73-1 Sample IES configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies by access interfaces is defined when you configure or modify access interfaces during service creation or modification. The following key policies can be applied to resources that are part of an IES. • QoS access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the IP filter form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
2. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

3. Create and configure Service 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 9 for more information about user and user group privileges.
	Choose Create→Service→IES. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Choose Subscriber 1 as the customer for the IES.
	• Choose router 1 as the site for the IES.
	• Create and configure Access interface 1. You do the following to configure an access interface:
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign a transit IP or transit prefix policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Add unicast routing protocols as required.
	  • Assign ingress and egress QoS policies, as required.
	  • Add multicast routing protocols as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Specify one or more IP addresses for the IES access interface: one primary IP address and, optionally, multiple secondary IP addresses.
	  • Specify BFD parameters as required.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure IPCP parameters, if required.
	  • Configure ICMP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure ARP host configuration, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Create a MEP, if required.
	  • Configure router advertisement parameters.
	  • Create QoS policy overrides, if required.
	  • Configure ANCP parameters, if required.

(2 of 2)

73.3 Workflow to create an IES

The following workflow lists the high-level steps required to create an IES. As a prerequisite for creating a IES, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1.
- the access ports for the service are created; see chapter 20 for more information.

- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.

1 Create the IES. See Procedure 73-1.

i Choose a customer to associate with the IES.

ii Define the general properties for the IES.

iii Choose a router as the IES site.

iv Create an L3 access interface.

v Apply policies to the IES as required.

vi Turn up the IES service.

2 Perform one or more of the following.

a Apply routing protocols, such as OSPF, RIP, or IS-IS, to an IES site, if required. See Procedure 73-2.

b Apply routing protocols, such as OSPF, RIP, or IS-IS, to an IES L3 interface, if required. See Procedure 73-3.

c Add an IGMP interface to an IES. See Procedure 73-4.

d Add a PIM interface to an IES. See Procedure 73-5.

e Create an L2 SDP spoke termination on an IES service. See Procedure 73-6.

f Add a subscriber interface to an IES. See Procedure 73-7.

g Add a group interface to an IES. See Procedure 73-8.

h Configure a GNE site on an IES service. See Procedure 73-9.

i Implement dual homing using SRR. See Procedure 73-10.

j Create and enable a video interface for the IES site, if required. See Procedure 36-2.

3 As required, view IES information:

a View the IES service operational status. See Procedure 73-11.

b View the service topology map associated with an IES. See Procedure 73-12.

4 As required, modify a IES:

a Using the Manage Services form. See Procedure 73-13.

b Using the topology view. See Procedure 73-14.

5 As required, delete an IES. See Procedure 73-15.

73.4 IES management procedures

Use the following procedures to perform IES creation and management tasks.

Note — To configure a port in the 7210 SAS-M access uplink mode see Procedure 73-1. The 7210 SAS-M does not support IES in Network mode.

Procedure 73-1 To create an IES

1. Choose Create→Service→IES from the 5620 SAM main menu. The IES Service (Create) form opens with the General tab displayed.

2. Click on the Select button to choose a customer to associate with the IES. The Select Customer - IES Service form opens.

3. Select a customer for the IES and click on the OK button. The Select Customer - IES Service form closes, and the IES Service (Create) form reappears with the customer information displayed in the Customer panel.

4. Configure the parameters:

   - Service ID
     This parameter is configurable when the Auto-Assign ID parameter is disabled.
   - Auto-Assign ID
   - SVC Mgr Service ID
     This parameter is configurable when the Auto-Assign ID parameter is disabled.
   - Service Name
   - Description
   - Service Tier
   - Service Prioirity
   - Administrative State
   - OLC State
     This parameter is configurable when you click on the Apply button.

5. To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

   i. Click on the 5670 RAM Parameters tab button.

   ii. Click on the General tab button.

   iii. Configure the parameters:

      - Enable Application Performance Reporting
      - Report Customer Name

6 Perform one of the following:

a Create a site for the IES. Go to step 7.

b Complete service creation if sites and access interfaces for the IES are to be created later. Go to step 61.

For information on adding a GNE site to an IES service, see Procedure 73-9.

7 On the navigation tree, right-click IES Service and choose Create IES Site. The Select Network Elements - IES Service form opens with a list of available sites.

8 Select a site and click on the OK button. The IES Site (Create) form opens with general information about the site displayed in the Network Element panel.

9 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

10 Click on the IGMP Host Tracking tab button.

11 Configure the parameters:

- Administrative State
- Expiry Time

12 Perform one of the following steps.

a Create an access interface for the site. Go to step 13.

b Complete site creation if access interfaces for the site are to be created later. Go to step 54.

13 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

14 RIght-click on Access Interfaces and choose Create IES L3 Access Interface. The IES L3 Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Class
- Trusted
- IPv6 Allowed
- Admin Link Local Address
- Admin Link Local Address Preferred
- FlowSpec Validate Enabled
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Calling Station ID
- Configured IP MTU (Octets)
- Unnumbered Type
- IP Address
- Interface Name
- URPF Check State
- URPF Check Mode
- Tunnel Fault Notification

Note 1 — The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

Note 2 — The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

Note 3 — The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

Note 4 — The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

Note 5 — The FlowSpec Validate Enabled parameter is available only when a port is configured on the interface. You may have to complete steps 23 to 27 before configuring this parameter.

Note 6 — The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

16 If the Loopback Enabled parameter in step 15 is enabled, you cannot associate a port with the L3 interface. Go to step 40.

17 Bind an application profile to the IES L3 access interface, if required:

i Click on the Select button beside the Application Profile parameter in the Application Assurance panel. The Application Profile String: - IES L3 Access Interface list form opens.

ii Select a profile from the list and click on the OK button. The Application Profile String - IES L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.

Note — The Application Profile String: - IES L3 Access Interface list form only displays local profiles that already exist on the NE.

18 Choose one of the following AA transit policy types, if required.

Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Select a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

19 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab button.

20 Configure Unicast RPF if required.

- URPF Check State
- URPF Check Mode

Note — The URPF Check State parameter must be enabled to display the URPF Check Mode parameter.

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The IES L3 Access Interface (Create) form closes, and the IES Site (Create) form displays the new access interface.

23 Click on the Port tab button.

24 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - IES L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

25 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form displays the port information.

26 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

27 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle was selected in step 25, only the Scheduling Class parameter are configurable.

28 Bind an IES L3 access interface to a VPLS site, if required.

Note 1 — The operational state of the IP interface binding will not be turned up until the parameter Enable IP Interface Binding is set to true.

Note 2 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form.

i Click on the Routed VPLS tab button.

ii Enter a VPLS site name or click on the Select button next to the VPLS Name parameter to choose a VPLS site with a configured site name. The Routed VPLS String - IES L3 Access Interface form opens.

iii Select a VPLS site and click on the OK button. The VPLS site is displayed.

iv In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - IES L3 Access Interface form opens.

v Select an IPv4 filter and click on the OK button. The IPv4 filter information is displayed.

vi In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - IES L3 Access Interface form opens.

vii Select an IPv6 filter and click on the OK button. The IPv6 filter information is displayed.

viii In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - IES L3 Access Interface form opens.

ix Select a QoS Policy and click on the the OK button. The QoS Policy information is displayed.

29 Some devices support the application of QoS and accounting policies, queue schedulers, ANCP policies, ACL filters to interfaces and associating a local DHCP server.

a If your device supports these functions, go to step 30.

b If your device does not support these functions, the QoS, Schedulers, ACL, ANCP policies, Local DHCP server and Accounting tabs are not present. Go to step 40.

30 Assign ingress and egress QoS policies to the interface, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

i Click on the QoS tab button.

Note — The QoS tab is configurable only when a port is assigned to the interface.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID
- Use Multipoint Shared Queue

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - IES L3 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port selected in step 25 uses the same access ingress queue group.

See Procedure 20-1 in chapter 20 for information about configuring Ethernet ports. See chapter 46 for information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - IES L3 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the egress QoS policy information displayed.

Note — If you select an egress policy that has a forwarding class mapped to an egress queue group, you must ensure that the port selected in step 25 uses the same access egress queue group.

See Procedure 20-1 in chapter 20 for information about configuring Ethernet ports. See chapter 46 for information about queue group template policies.

vii If you are configuring an L3 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 25 is not an HSMDA port, then go to step 31.

viii Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

ix Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

x Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the IES L3 Access Interface (Create) form reappears with the WRR policy information displayed.

xi Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xii Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the IES L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

31 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 33.

Note — The Schedulers tab is configurable only when a port is assigned to the interface.

32 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

Note — The Aggregation parameter is not configurable if the port you selected in step 25 is an HSMDA port.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 25 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES L3 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the IES L3 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 25 is an HSMDA port, go to step 33.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES L3 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the IES L3 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 33.

b Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

Note — You cannot specify an access scheduler policy if the port you selected in step 25 is an HSMDA port. Go to step 33.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES L3 Access Interface form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

33 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - IES L3 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - IES L3 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - IES L3 Access Interface form opens.

vii Select an ingress IPv6 ACL filter and click on the OK button. The Select IPv6 Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress IPv6 ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - IES L3 Access Interface form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

34 To associate a local DHCPv4 or DHCPv6 server to the IES L3 interface, if required, click on the Local DHCP tab button and perform one of the following steps.

Note — To associate local DHCPv6 servers the IPv6 Allowed parameter must be enabled.

a For local DHCPv4 servers

i Click on the Select button in the Local DHCP Server panel to choose a local DHCP server. The Select Local DHCP Server - IES L3 Access Interface form opens.

ii Select a local DHCP server and click on the OK button. The Select Local DHCP Server - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the local DHCP server information displayed.

b For local DHCPv6 servers

Note — You cannot associate a local DHCPv4 server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up. Go to step 47 to set the Administrative State.

i Click on the Select button in the Local DHCPv6 Server panel to choose a local DHCPv6 server. The Select Local DHCPv6 Server - IES L3 Access Interface form opens.

ii Select a local DHCPv6 server and click on the OK button. The Select Local DHCPv6 Server - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the local DHCPv6 server information displayed.

Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

35 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES L3 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the accounting policy information displayed.

36 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

37 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - IES L3 Access Interface list form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - IES L3 Access Interface list form closes, and the IES L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the L3 access interface. You must first disable the Collect Accounting Statistics parameter in step 35.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

38 Configure residential subscriber management for the interface, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step 39.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

iv Click on the Profiles tab button. If the Profiles tab is not enabled, go to step 39.

v Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- LAG link selection

39 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - IES L3 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - IES L3 Access Interface form closes and the policy ID is displayed on the IES L3 Access Interface (Create) form.

40 Assign an IP address to the interface.

i Click on the Addresses tab button.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

Note 1 — The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

Note 2 — The EUI-64 IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

Note 3 — The secondary IP addresses must not overlap with the primary IP address.

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IES L3 Access Interface (Create) form reappears with the assigned IP addresses displayed.

41 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button.

ii Click on the Configuration tab button.

iii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier

iv To view local and remote session peers, click on the BFD Session tab button. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties form opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

vi Click on the OK button.

Note 1 — You cannot enable BFD on an interface if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled when protocols using the interface have BFD enabled. See chapter 31 for information about enabling and disabling BFD for routing protocols.

Note 2 — If the IPv6 Allowed parameter in step 15 is enabled, you can configure the above BFD parameters for IPv6.

42 Configure IPv4 ICMP for the interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

43 If the IPv6 Allowed parameter in step 15 is enabled, the ICMPv6 tab is configurable. Configure IPv6 ICMP, if required. Otherwise, go to step 44.

Configure the parameters:

- Redirects
- Unreachables
- Packet Too Big
- Param Problem
- Time Exceeded
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Number of Param Problem
- Param Problem Time (seconds)
- Number of Time Exceeded
- Time Exceeded Time (seconds)

44 Configure IPCP for the interface, if required. IPCP is available only on the ASAP MDA of 7750 SR, and 7710 SR.

i Click on the IPCP tab button.

ii Configure the parameters:

- Peer Address
- Primary DNS Address
- Secondary DNS Address

Note — Primary and secondary DNS addresses have similar functionality. However, they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to confirm the action.

The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

45 Configure ARP for the interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii To add a static ARP entry, click on the Create button. The Static ARP (Create) form opens.

iv Configure the parameters:

- IP Address
- Physical Address

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Static ARP (Create) form closes, and the General tab refreshes with the configured static hosts displayed in a list.

vii Repeat steps iii to vi to create additional entries, if required.

viii Click on the OK button. A dialog box appears.

ix Click on the Proxy ARP tab button.

x Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

46 If the IPv6 Allowed parameter in step 15 is enabled, the Neighbor Discovery tab is configurable. Configure neighbor discovery, if required. Otherwise, go to step 47.

i Click on the Neighbor Discovery tab button.

ii Click on the Create button. The Neighbor Discovery (Create) form opens.

iii Configure the parameters:

- IP Address
- Physical Address

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Neighbor Discovery (Create) form closes, and the IES L3 Access Interface (Create) form refreshes with the neighbor entry.

vi If the Proxy ND tab is present, click on the Proxy ND tab button. Otherwise, go to step viii.

vii Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 1
- Policy 5

Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured, or the 5620 SAM reorders the policies and move the policy specified for the Policy 3 parameter to the Policy 2 parameter.

viii Repeat steps i to vii for each neighbor entry you want to create.

47 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

Note — The Lease Populate parameter is configurable when the Enable parameter is enabled.

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step viii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

v Configure the filter criteria.

vi Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the L3 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source

Note — The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

viii Click on the Server tab button.

ix Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

48 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the L3 Access Interface (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the L3 Access Interface (Create) form refreshes with the egress ATM policy information displayed.

49 Click on the VRRP tab button to create a VRRP instance on the current L3 interface for a virtual router. You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- Two sub-tabs are available under the VRRP tab, one for IPv4 instances and the other for IPv6 instances. You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter in step 15.
- The Link Local Address on the parent interface has to be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. To do this, the Admin Link Local Address and Admin Link Local Address Preferred parameters in step 15 must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 40 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 51 for the router advertisement on the parent interface.

See chapter 39 for additional configuration information about VRRP instances and virtual routers.

i Click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed.

ii Configure the Virtual Router ID parameter.

iii Perform steps 8 to 15 of Procedure 39-2.

Note — You can use the VR Instances tab to create, modify, and view VR instances.

iv Click on the OK button. The VRRP Instance (Create) form closes and the L3 Access Interface- Subscriber (Create) form reappears.

50 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Populate

Note — The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

iii Click on the Static Hosts tab button to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management. Otherwise, go to step 54.

iv Click on the Create button. The Access Interface Anti-Spoofing Static Host (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address

Note 1 — At least one IP address or MAC address must be specified for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

Note 2 — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

Note 3 — When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in step 40.

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes, and the Static Hosts tab refreshes with the configured static hosts displayed in a list.

51 Configure router advertisement, if required.

i Click on the Advertisement tab button.

ii Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens.

iii Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

Note — If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

iv Click on the Prefix tab button.

v Click on the Create button. The Router Advertisement Prefix (Create) form opens.

vi Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

Note — Each Lifetime (seconds) parameter is configurable when the associated No Expiry parameter is disabled.

52 Click on the OK button. A dialog box appears.

53 Click on the OK button. The Router Advertisement Prefix (Create) form closes.

54 Click on the OK button. A dialog box appears.

55 Click on the OK button. The IES L3 Access Interface (Create) form refreshes with the router advertisement entry.

56 Specify queue overrides by clicking on the Override Policy Items tab button.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

Set the queue overrides, as described in Procedure 47-44.

57 If the IPv6 Allowed parameter in step 15 is enabled, the DHCPv6 tab is configurable. Configure IPv6 DHCP, if required. Otherwise, go to step 20.

i Click on the DHCPv6 tab button. The DHCPv6-Prefix tab is displayed.

ii Click on the Create button. The DhcpRelayV6PrefixDelegation (Create) form opens.

iii Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L3 Access Interface (Create) form reappears.

vi Click on the DHCPv6-Relay tab button.

vii Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

viii Click on the Server tab button.

ix Configure the Server 1 through Server 8 parameters.

x Configure the interface name for each DHCPv6 server that you configured in step ix by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

xi Select an interface from the list and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the L3 Access Interface form refreshes with the interface information.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The L3 Access Interface (Create) form reappears.

58 Add a Video interface to the IES site, if required. See Procedure 36-2 for more information.

59 Click on the OK button. The IES Site (Create) form closes, and the IES Service (Create) form reappears with the new site information displayed in the service navigation tree.

60 Perform one of the following steps.

a Create an additional site for the IES. Go to step 7.

b Complete service creation. Go to step 61.

61 Click on the OK button. A dialog box appears.

62 Click on the Yes button to confirm the action. The IES Service (Create) form closes.

Procedure 73-2 To apply OSPF, RIP, or IS-IS to an IES

Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES in the list and click on the Properties button. The IES Site (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Protocols tab button.

7 Click on the Create button. The Create Interface form opens.

8 Specify the interface type by configuring the What type of interface would you like to create? parameter.

9 Click on the OK button. The Interface (Create) form opens. See section 31.2 for information about configuring specific routing protocols.

Procedure 73-3 To apply OSPF, RIP, or IS-IS to an IES L3 interface

Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an L3 interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria.A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the L3 Access Interfaces tab button.

5 Select an L3 interface in the list and click on the Properties button. The L3 Access Interface (Edit) form opens.

6 Click on the Protocols tab button.

7 Click on the Create button. The Create Interface form opens.

8 Specify the interface type by configuring the What type of interface would you like to create? parameter.

9 Click on the OK button. The Interface (Create) form opens. See section 31.2 for information about configuring specific routing protocols.

Procedure 73-4 To add an IGMP interface to an IES

Note — IGMP must be enabled on the NE routing instance before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Multicast tab button.

7 Click on the Interfaces tab button.

8 Click on the Create button. The Create Interface form opens.

9 Set the What type of interface would you like to create? parameter to IGMP.

10 Click on the OK button. The IGMP Interface (Create) form opens with the General tab displayed.

11 Click on the Select button to specify an interface. The Select Interface form opens.

12 Click the Search button. A list of interfaces appears at the bottom of the Select Interface form.

13 Select an interface and click the OK button. The Select Interface form closes and the Interface panel refreshes with the interface parameters.

14 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

15 Click on the Behavior tab button.

16 Configure the Import Policy parameter.

17 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Select Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

19 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form appears.

20 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

21 Click on the Static Group/Source tab button to add a static multicast group or source, if required.

22 Click on the Create button to add a new entry. The StaticGrpSrc, Interface ID - 6, Routing Instance (Create) form opens.

23 Configure the parameters:

- Static Multicast Group
- Static Source

24 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

25 Click on the OK button to confirm the action. The IGMP Interface, Routing Instance (Create) form reappears.

26 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form.

27 Click on the OK button to close the IGMP Interface (Create) form.

28 Click on the Group Interfaces tab button to identify an IGMP group interface for the IES service, if required.

29 Click on the Create button and configure the parameters in the IGMP Group Interface - Routing Instance (Create) form:

- Description
- Administrative State
- Name

30 Click on the Select button next to the Interface ID field to select a group interface from the Select IGMP Group Interface - IGMP Group Interface - Routing Instance form.

31 Click on the OK button to close the Site (Edit) form.

32 Click on the OK button to close the IES (Edit) form. A dialog box appears.

33 Click on the Yes button to confirm the action. The IES (Edit) form closes.

34 Close the Manage Services form.

Procedure 73-5 To add a PIM interface to an IES

Note — Before you can add a PIM interface to an IES, PIM must be applied to All or IES during the PIM configuration at the routing instance level. See Procedure 31-33 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES in the list and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Multicast tab button.

7 Click on the Create button. The Create Interface form opens.

8 Set the What type of interface would you like to create? parameter to PIM.

9 Click on the OK button. The PIM Interface (Create) form opens with the General tab displayed.

10 Click on the Select button to specify an interface. The Select Interface - PIM Interface form opens.

11 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

12 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

13 Configure the parameters:

- Description
- Administrative State
- Administrative State IPv4
- BFD Enabled
- IPv6 BFD Enabled

14 Click on the Behavior tab button.

15 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Sticky DR Priority

Note — The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

16 Click on the Neighbor tab button, if present, to view and edit information. The Neighbor tab is present only when a neighbor PIM interface exists.

17 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

19 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form reappears.

20 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

21 Click on the IPv6 Specifics tab button.

22 Configure the IPv6 Administrative State parameter.

23 Click on the OK button to close the PIM Interface (Create) form.

24 Click on the OK button to close the IES Site (Edit) form.

25 Click on the OK button to close the IES Service (Edit) form. A dialog box appears.

26 Click on the Yes button to confirm the action. The IES Service (Edit) form closes.

27 Close the Manage Services form.

Procedure 73-6 To create an L2 SDP spoke termination on an IES service

Ensure that a service and site have been created in the IES. To terminate an L2 service on an IES SDP spoke, you must identify the VC and an interface belonging to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site to which you want to add the L2 SDP spoke termination; expand the entries for that site.

5 Right-click on Spoke Sdp Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the spoke SDP binding.

i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of source interfaces appears at the bottom of the Select Source Interface - Spoke SDP Binding form.

iii Choose a source interface from the list and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

7 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element form opens.

ii Select a destination node and click on the OK button. The Select Destination Network Element form closes, and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

8 Configure the parameters:

- Description
- VC ID
- VC Type
- Auto-Assign ID
- Ingress Label
- Egress Label
- Enable Hash Label
- FlowSpec Validate Enabled
- Enable Signal Capability

The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated.

9 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Specify an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - IES service form displays only local profiles on the NE.

11 Choose one of the following AA transit policy types, if required.

Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Select a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

12 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab button.

13 Click on the States tab button.

14 Configure the Administrative State parameter.

15 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

16 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

17 Associate a MEP with an SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 18.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

18 Click on the OK button. The MEP (Create) form closes.

19 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

20 Click on the OK button. The IES Service (Edit) form reappears with the new information displayed in the service navigation tree.

Procedure 73-7 To add a subscriber interface to an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service Subscriber (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the subscriber interface; expand the entries for that site.

5 Right-click on the Subscriber Interfaces icon below the site to which you want to add the subscriber interface, and choose Create IES Subscriber Interface. The IES Subscriber Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address
- Tunnel Fault Notification

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

Note 1 — The Name value for a subscriber interface must be unique in the NE.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

7 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed and IPv6 Delegated Prefix Length parameters.

- IPv6 Allowed
- IPv6 Delegated Prefix Length
- Admin Link Local Address

The Admin Link Local Address parameter is only configurable when the IPv6 Allowed parameter is enabled.

ii Click on the IPv6 Subscriber Prefixes tab button.

iii Select a subscriber prefix from the list and click on the Properties button, or click on the Create button to create a new subscriber prefix.

iv In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

8 Configure the Interface Class parameters, if required.

i Configure the Class parameter.

ii If you selected a value of Unnumbered for the Class parameter, configure the Unnumbered Type parameter.

iii Configure the Interface Name parameter or the IP Address parameter.

9 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Addresses tab button.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Track SRRP Instance
- Hold Up Time (milliseconds)
- Gateway IP Address
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IES Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you want to create.

10 Click on the DHCP tab button.

11 Configure the parameters:

- IP address
- Use as source

12 Click on the OK button. The IES Subscriber Interface (Create) form closes, and a dialog box appears.

13 Click on the OK button. The IES Service (Edit) form reappears with the new subscriber interface displayed in the service navigation tree.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The IES Service (Edit) form closes, and the Manage Services form reappears.

16 Close the Manage Services form.

Procedure 73-8 To add a group interface to an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the group interface; expand the entries for that site.

5 Right-click on the subscriber interface to which you want to add a group interface, and choose Create IES Subscriber Interface. The IES Subscriber Interface (Create) form opens with the General tab displayed.

6 Click on the Group Interfaces tab button.

7 Click on the Create button. The IES Group Interface (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- Operational State UP While Empty
- LNS
- IPv6 Allowed
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6

Note — The LNS parameter defines the type of group interface. This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes, and an LNS group interface does not allow PPPoE configuration or SAPs.

9 Configure IPv6 router advertisement and DHCPv6 on the group interface, if required.

i Configure the IPv6 Allowed parameter.

ii Click on the IPv6 Advertisement tab button and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Life Time
- Valid Life Time

iii Click on the DHCPv6 tab button.

iv Click on the Select button and select a local user database from the Select Local User Database form.

v Click on the Proxy Server tab button and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Life Time
- Preferred Life Time
- Client Applications

vi Click on the Relay tab button and configure the parameters:

- Administrative State
- Description
- Remote ID
- Client Applications

vii Configure the DHCP Server 1 through DHCP Server 8 parameters:

- Server 1 through Server 8
- Configure the interface name for each DHCPv6 server by clicking on the Select button in the Zone Index panel. The Select Zone Index - GrplfDhcpv6RelayCfg form opens with a list of local L3 access interfaces and network interfaces.
- Select an interface from the list and click on the OK button. The Select Zone Index - GrplfDhcpv6RelayCfg form closes and the IES Group Interface form refreshes with the interface name.

Note — If you have entered a Unicast address, then the Interface Name parameter is not required.

10 Click on the Anti-Spoofing tab button.

11 Configure the ARP Populate parameter.

12 Click on the Subscriber Management tab button.

13 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

Note — The SHCV Interval (minutes), SHCV Source, and SHCV Action parameters are configurable only when the SHCV Enabled parameter is set to enabled.

14 Configure SRRP for the group interface, if required.

i Configure the parameters in the Routing panel:

- Enabled
- Hold Time (seconds)

ii Click on the SRRP tab button.

iii Click on the Create button in the SRRP Instance panel. The SRRP Instance (Create) form opens with the General tab displayed.

iv Configure the parameters:

- SRRP ID
- Description
- Administrative State

v Click on the Select button in the Operational Group panel. The Select Monitored Group Name - SRRP Instance form opens.

vi Select a Monitored Group Name and click on the OK button. The Select Monitored Group Name - SRRP Instance form closes.

vii Configure the Priority Step parameter.

viii Click on the Behavior tab button.

ix Configure the General parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- Preempt
- FIB Population Mode
- One Gratuitous ARP Per SAP

x Click on the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

xi Select the SAP you want to use for the in-band messaging between the sites and click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

xii Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens.

xiii Select an entry and click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

xiv Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 2 - SRRP Instance form opens.

xv Select an entry and click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

xvi Click on the OK button. The SRRP Instance (Create) form closes and a dialog box appears.

xvii Click on the OK button.

15 Configure ICMP for the group interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

16 Configure ARP for the group interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 5

17 Configure DHCP relay for the group interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof MAC Address

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Select Subscriber Authentication Policy, if required. Otherwise, go to step xiii.

iv Click on the Select button in the Subscriber Authentication Policy panel. The Select Subscriber Authentication Policy - GrpltfDhcpRelayCfg form opens.

v Configure the filter criteria.

vi Click the Search button. A list of subscribers is listed.

vii Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - GrpltfDchpRelayCfg form closes, and the IES Group Interface (Create) form refreshes with the subscriber authentication policy name.

viii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source

Note — The Remote ID String parameter is configurable when the Remote ID is set to Remote IDString.

ix Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

x Configure the filter criteria.

xi Click the Search button. A list of available databases appears.

xii Select a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the IES Group Interface (Create) form reappears with the database name information displayed.

xiii Click on the Server tab button.

xiv Configure the parameters:

- Server 1 to Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

18 Click on the Client Applications tab button. Configure the Client Applications parameter.

19 Click on the PPP tab button.

20 Configure the Description and Administrative State parameters.

21 Click on the Select button in the PPPoE Policy panel. The Select PPPoE Policy form opens.

22 Select a PPPoE policy from the list and click on the OK button. The Select PPPoE Policy form closes.

23 Click on the Select button in the PPPoE Local User DB panel. The Select PPPoE Local User DB form opens.

24 Select a PPPoE Local User DB from the list and click on the OK button. The Select PPPoE Local User DB form closes.

25 Click on the Select button in the PPP Policy panel. The Select PPP Policy form opens.

26 Select a PPP policy from the list and click on the OK button. The Select PPP Policy form closes.

27 Click on the Select button in the PPP Local User DB panel. The Select PPP Local User DB form opens.

28 Select a PPP Local User DB from the list and click on the OK button. The Select PPP Local User DB form closes.

29 Configure the remaining parameters:

- Session Limit
- Session Limit per SAP

30 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)
- SAP ARP Host Limit

31 If you set the parameter LNS to TRUE in step 8, perform the following steps to configure LNS for the group interface.

Note — After you create an LNS group interface, you must configure the L2TP tunnel group profile or L2TP tunnel profile to terminate sessions for the LNS group interface; see Procedure 31-30 for more information. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab button.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens.

iv Select a subscriber profile from the list and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens.

vi Select an SLA profile from the list and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens.

viii Select a subscriber identification policy from the list and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens.

x Select a default application profile from the list and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the default application profile displayed.

32 Configure the Default Subscriber Identification String parameter.

33 Click on the Service Access Points tab button to configure SAPs for the group interface.

34 Click on the Create button. The IES Service Access Point (Create) form opens with the General tab displayed.

35 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

36 Click on the Port tab button.

37 Click on the Select button to choose a port for the SAP. The Select Terminating Port - IES Service Access Point form opens.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 68-25 for more information about deleting MSAPs.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

38 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES Service Access Point form closes, and the IES Service Access Point (Create) form displays the port information.

39 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses dot1q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

40 Assign ingress and egress QoS policies to the SAP, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service navigation tree, choose Properties, and configure the parameters on the appropriate tab. This action opens a properties form in a new window for the component that was right-clicked. The navigation tree is not displayed in this new window.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID

iii Click on the Select button in the Ingress Policy panel. The Select Ingress Policy - IES Service Access Point form opens.

iv Configure the filter criteria and click on the Search button. A list of available ingress policies appear.

v Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES Service Access Point form closes, and the IES L3 Service Access Point (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 38 has the access ingress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

vi Click on the Select button in the Egress Policy panel. The Select Egress Policy - IES L3 Service Access Interface form opens.

vii Configure the filter criteria and click on the Search button. A list of available egress policies is displayed.

viii Select an egress QoS policy and click on the OK button. The Select Egress Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the egress QoS policy information displayed.

Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 38 has the access egress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

41 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 43.

Note — The Schedulers tab is displayed only if a port is assigned to the SAP earlier in the procedure.

42 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 38 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are displayed only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 38 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES Service Access Point form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

vi Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 38 is an HSMDA port, go to step 43.

viii Click on the Select button in the Select Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES Service Access Point form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xi Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 43.

b Specify that an aggregation scheduler policy is applied to the SAP.

Note — You cannot specify an access scheduler policy if the port you selected in step 38 is an HSMDA port. Go to step 43.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES Service Access Point form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

43 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - IES Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - IES Service Access Point form.

44 Click on the Accounting tab button to assign an accounting policy to the SAP.

i Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES Service Access Point form opens.

ii Select an accounting policy and click on the OK button. The Select Accounting Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the accounting policy information displayed.

iii Configure the Collect Accounting Statistics parameter.

45 Click on the Anti-Spoofing tab button to configure anti-spoofing for the SAP. The Anti-Spoofing tab opens with the General tab displayed.

i Configure the Anti-Spoofing parameter.

ii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iii Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

iv Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

v Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed.

vi Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

vii Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

viii Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

ix Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

x Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

46 Assign a DoS protection policy to the SAP, if required.

Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - IES Service Access Point form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - IES Service Access Point form closes and the Policy ID is displayed on the IES Service Access Point (Create) form.

iv Configure the MAC Monitoring parameter.

47 Associate a MEP to the SAP, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

48 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 52.

49 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

50 Click on the AIS tab button.

51 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

52 Click on the OK button. The MEP (Create) form displays the SAP information.

53 Click on the OK button. The MEP (Create) form closes.

54 Click on the Subscriber Management tab button to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group
- Disable Router Alert Check

v You can click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab button.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Select a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Select an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Select a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Select an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Select a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Select an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Select an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

55 Assign an ANCP policy to the SAP, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

56 Configure ATM on the SAP, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the IES Service Access Point (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the IES Service Access Point (Create) form refreshes with the egress ATM policy information displayed.

57 Modify PPPoE Sessions that have been generated by the NE, for the group interface, if required. See chapter 68 for more information about viewing and configuring a PPPoE session.

58 Click on the OK button. The IES Service Access Point (Create) form closes, and a dialog box appears.

59 Click on the OK button. The IES Group Interface (Create) form refreshes to display the SAP.

60 To configure additional SAPs in the group interface, go to step 34.

61 Click on the OK button. The IES Group Interface (Create) form closes, and a dialog box appears.

62 Click on the OK button. The IES Service (Edit) form refreshes to display the SAP below the group interface.

63 Click on the OK button. A dialog box appears.

64 Click on the Yes button. The IES Service (Edit) form closes.

65 Close the Manage Services form.

Procedure 73-9 To configure a GNE site on an IES service

Use this procedure to add a GNE site and GNE service interfaces to an existing IES service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select an IES service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on IES Service and choose Create GNE Site. The Select Network Elements - IES Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab button and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab button and then click on the Select button next to the Interface Index field. The Select Generic NE Interface form appears.

iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encap Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab button to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The IES (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The IES (Edit) form closes.

You can use the topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 73-10 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Specify the pair of sites that are to participate in dual homing.

Note — The sites can be from different services.

5 Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that will be participating in the redundant configuration.

6 Ensure that all subscriber interface IP addresses have a gateway address configured on them.

7 Create the Redundant Interface (used for SRRP out-of-band messaging) between the two routers.

i On the navigation tree, click on the site; expand the entries for that site.

ii Right-click on the Redundant Interfaces item for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iv Click on the Addresses tab button.

v Click on the Create button. The IP Address (Create) form opens.

vi Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address (in the form d.d.d.d, where d is a value from 0 to 255)
- Prefix Length
- Remote IP Address
  This must be on the same subnet as the current site's redundant interface IP Address. For example, if the current site's IP Address is 7.7.7.7, with a Prefix Length of 24, then the remote site's redundant interface address must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.
- Broadcast Address Format

vii Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

viii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses displayed.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Redundant Interface (Create) form for the current site closes.

8 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 7 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site.

9 Assign the Redundant Interface to the Group Interface for the current site.

i On the navigation tree under Subscriber Interfaces, right-click on the group interface you want to use and choose Properties. The IES Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface panel. The Select Redundant Interface - IES Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of redundant interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 7 and click on the OK button. The Select Redundant Interface - IES Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The IES Group Interface (Edit) form closes.

10 Create an SRRP Instance for the current site.

i On the navigation tree under group interfaces, right-click on the SRRP Instances item for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
  The SRRP ID must be the same value for both the current and remote sites.
- Description
- Administrative State

iii Click on the Behavior tab button.

iv Configure the parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- FIB Population Mode

v Configure the message path by clicking the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

vi Select the SAP you want to use for the in-band messaging between the sites.

- **vii** Click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.
- **viii** Configure policy pointer 1, if required, by clicking the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens, displaying the pointers available on the site.
- **ix** Select the pointer you want to use.
- **x** Click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.
- **xi** Configure policy pointer 2, if required, by clicking the Select button in the Policy Pointer 2 panel. The Select Policy Pointer 2 - SRRP Instance form opens, displaying the pointers available on the site.
- **xii** Select the pointer you want to use.
- **xiii** Click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.
- **xiv** Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.
- **xv** Click on the OK button. The IES (Edit) form reappears with the SRRP Instance displayed.

11 Click on the Turn Up button to activate the SRRP instance.

12 Repeat steps 7 to 11 for the remote site.

Note 1 — When you repeat steps 7 to 11 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's navigation tree. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote node.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The IES (Edit) form closes.

Procedure 73-11 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The IES Service (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the IES Service (Edit) form.

9 Close the Manage Services form.

Procedure 73-12 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - map opens.

See chapter 5 for more information about service topology views.

Procedure 73-13 To modify an IES

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- General tab — displays general customer and service information
- Sites tab — lists the sites that are included in the service
- L3 Access Interfaces tab — lists the L3 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Addresses tab — lists the IP addresses that are associated with the service

  Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Subscriber Interfaces tab — allows the creation and configuration of subscriber and group interfaces for L3 aggregation
- Redundant Interfaces tab — allows the creation and configuration of redundant interfaces
- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The IES Service (Edit) form closes, and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 73-14 To modify an IES using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains two sub-procedures describing the components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating spoke SDP bindings. Go to step 9.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create IES Site option.

The Select Network Elements form appears.

5 Select one or more sites to add to the service and click OK. The IES Site (Create) form for the new site is displayed. If you selected more than one site, the IES Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The IES Site (Create) (or IES Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedure 73-1 for detailed site configuration information.

8 Go to step 9 if you want to create spoke SDP bindings or go to step 16 to finish.

Creating spoke SDP bindings

9 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

10 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

11 Enable the Auto-Select Transport Tunnel parameter.

12 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 73-6 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

13 Assuming that the spoke SDP binding was successfully created in step 12, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

14 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

15 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

16 Close the Service Topology form.

17 Close the Manage Services form.

Procedure 73-15 To delete an IES

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

  a For services with a low priority, go to Step 5.

  b For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.

  c For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

74 — VPRN service management

74.1 VPRN service management overview

The 5620 SAM supports the creation of VPRN services using the 7450 ESS in mixed mode, 7750 SR and 7710 SR as a PE and provider core (P) router. VPRNs, also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis. This standard describes a method of forwarding data and distributing routing information across an IP/MPLS service provider core network.

The 5620 SAM does not support the configuration of CE routers or devices.

VPRN services use BGP to exchange the VPRN routes among the PE routers that participate in the VPRN. This is done in a way that ensures that routes from different VPRNs remain distinct and separate, even if two VPRNs have an overlapping address space. PE routers distribute routes to CE routers in the VPRN. Since the CE routers do not peer with each other, there is no overlay visible to the VPRN's routing algorithm. The PE routers use BGP, RIP, or OSPFv2 as the IGP to distribute internal routes to the CE routers.

Each route in a VPRN service is assigned an MPLS label. When BGP distributes a VPRN route, it also distributes an MPLS label for that route. Before a customer data packet travels across the backbone network, it is encapsulated with the MPLS label that corresponds, in the customer VPRN, to the route that best matches the destination address of the packet.

The MPLS packet is further encapsulated with either another MPLS label or with an IP or GRE tunnel header, so that it gets tunneled across the backbone to the proper PE router. Each route exchanged by the MP-BGP protocol includes an RD that identifies the VPRN association. Thus the backbone core routers do not need to know the VPRN routes.

The 5620 SAM supports end-to-end VPRN configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in a VPRN of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 68 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 256 subnets. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays VPRN subscriber interfaces, group interfaces, and the associated SAPs.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT implementation in a VPRN service requires a NAT configuration on the VPRN routing instance and a NAT policy that is associated with a subscriber profile. See chapter 30 for general information about configuring and deploying NAT. See chapter 46 for information about configuring a NAT policy. See chapter 68 for information about associating a NAT policy with a subscriber profile. See Procedure 74-1 for information about configuring NAT on a VPRN routing instance.

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. See Procedure 74-13 for more information on how to define a wholesale and retail VPRN configuration.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

The 5620 SAM provides OAM tools for service validation and for troubleshooting service and network transport issues. You can run an OAM Validation test suite for the service by clicking on the More Actions > Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. The Validation Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 38 for general information about fault management using OAM tools. See chapter 78 for more information about how to configure OAM validation test suites.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When the Aggregated Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 76 for more information about the hierarchical organization of composite services.

Common to all device services, such as VPRN, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.

See chapter 46 for more information about policies.

VPRN service routers

A VPRN service consists of CE routers or devices connected to PE routers. PE routers connected to P routers transport data across the IP/MPLS provider core network in service tunnels.

Packets that arrive at an edge 7450 ESS, 7710 SR or 7750 SR are associated with a VPRN service based on the access interface on which they arrive. An access interface is uniquely identified by the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

Table 74-1 describes the general functions performed by PE, P, and CE routers in a VPRN. See Figure 74-4 in this chapter for a sample VPRN. See the appropriate hardware services guide for more detailed information about VPRN functionality on the supported managed devices.

Table 74-1 VPRN router functionality

Router type	Functionality
PE	• Are directly connected to PE, CE, and P routers • Learn VPRN routes from CE devices using e-BGP, RIP, OSPFv2, or static routes • Maintain a separate routing table, called a VRF, for each service • Exchange multicast VPRN route information with PE routers in other autonomous systems using MP-BGP • Distribute MPLS inner labels using MP-BGP. Before data traverses the IP/MPLS backbone, it is encapsulated with the MPLS label that corresponds, within the VPRN, to the route that best matches the packet's destination address. • Distribute MPLS outer labels using RSVP-TE or LDP. Before the MPLS packet traverses the IP/MPLS backbone, it is further encapsulated with either another MPLS label or with a GRE or MPLS LSP service tunnel header, so that it is tunneled across the backbone to the appropriate PE router. • Use RDs to identify the VPRN associations • Use RTs to determine when a received route is destined for a VPRN • Terminate RFC 2684-encapsulated IPv4 traffic from ATM access network on SAPs
P	• Are directly connected to PE and P routers • Act as transit LSRs • Maintain routes to PE routers and are unaware of specific VPRN routing information
CE	• Are directly connected to PE routers • Provide customer access to the VPRN

Inter-AS connections

You can connect VPRN service sites (or VRFs) on multiple ASs using EGBP. ASs set up mutual connections by exchanging routing information, such as routes and labels. Labeled VPN-IPv4 routes are distributed within an AS on a PE router using IGBP and between ASs using EGBP on an ASBR. The ASBR redistributes VPN-IPv4 routes to an ASBR in another AS, which in turn distributes the routes to PE routers in its own AS or to an ASBR.

When a VPRN inter-AS connection is between two service providers, the ASs must be on private peering points. For an LSP to operate between ASBRs on the AS borders, EBGP peering must be set up between the ASBRs and MPLS label exchange must be supported. Furthermore, an LSP must run from a packet's ingress PE router to its egress PE router.

You can enable inter-AS connections from the BGP settings in Procedure 74-5.

MP-BGP Multicast IPv4

The MP-BGP multicast extension allows for a network topology that supports both multicast and unicast routing. Routes from the unicast routing table can be imported into the multicast routing table, and routes from the multicast routing table can be imported into the unicast routing table. An ASBR can be configured to advertise VPRN routes to peers in other ASs, redistributing unicast routes learned by BGP into MP-BGP routes, and MP-BGP routes into unicast routes. This configuration enables the support of the two sets of routing information.

The MP-BGP multicast extension specifies that BGP can exchange routing information for the multicast IPv4 address family within and between BGP ASs. All configurations entered in a multicast IPv4 address family for a BGP instance affect multicast services and are applied to the multicast routing table. See chapter 31 for more information about the configuration of BGP and the MP-BGP multicast extension.

IPv6 support

The 5620 SAM supports IPv6 configuration of the following functions in VPRN services on the 7710 SR and 7750 SR, and on the 7450 ESS in mixed mode:

- addressing for static routes, L3 access interfaces, and BGP peerings
- router advertisement, ICMP, DHCP, neighbor discovery, and ACL filtering

To configure IPv6 in a VPRN, you must first enable VPN IPv6 for BGP on the base routing instance of each device that acts as a site in the VPRN.

A customer can use an SNMP utility to manage the IPv6 objects in a VPRN service. SNMP mediation of VPRN objects requires the configuration of a community string on each site in the VPRN, regardless of the IP or SNMP version. SNMPv3 mediation of VPRN IPv6 objects, however, requires the additional configuration of an SNMP context for the VPRN using a CLI. See chapter 14 for information about configuring an SNMPv3 context for a VPRN.

PIM for VPRN

The PIM protocol can be applied to a VPRN service to create a private multicast distribution network. PIM uses an MDT group address to identify multicast traffic for the VPRN instance to prevent flooding of multicast packets to PE devices in the VPRN. VRFs with the same MDT address are members of that group and receive multicast traffic from each other. The MDT address cannot be in the SSM range.

By default, the PIM protocol only uses the information in the unicast routing table to determine the RPF interface. PIM can be configured to use the separate multicast and unicast routing tables built by MP-BGP to perform RPF lookups for multicast-capable sources to build and maintain distribution trees for multicast traffic forwarding. See chapter 31 for more information about configuring PIM to use multicast or unicast routing tables in RPF lookups.

Data-MDT

A data-MDT is a tunnel for high-bandwidth source traffic through the P-network to interested PE routers. Data-MDTs do not broadcast customer multicast traffic to all PE routers in a multicast domain.

Note — Data-MDTs are only supported for VPRN services.

Multicast data transmission from a CE router is typically delivered to all CE routers in the same multicast group. Some CE routers do not require the delivery of a specific multicast stream because there no downstream receivers for the multicast group. You can prune a PE router from the MDT if the router does not deliver multicast traffic to the attached CE routers. This task is beneficial for high-traffic multicast applications.

A data-MDT allows you to configure a traffic threshold in Kb/s. The 5620 SAM signals the data-MDTs when the bandwidth for the SSM group exceeds the configured threshold. The PE router sends an MDT join TLV, at 60 s intervals, over the default MDT to all PE routers. The routers respond with the following actions:

- PE routers that require the SSM group specified in the MDT join TLV; join the data-MDT used by the PE router to transmit the SSM group
- PE routers that do not require the SSM group specified in the MDT join TLV; do not join the data-MDT, pruning the PEs from the MDT

The transmitting PE router switches the multicast stream to the data-MDT after allowing the PE routers to join the data MDT. You can configure the data-MDT delay interval using the 5620 SAM.

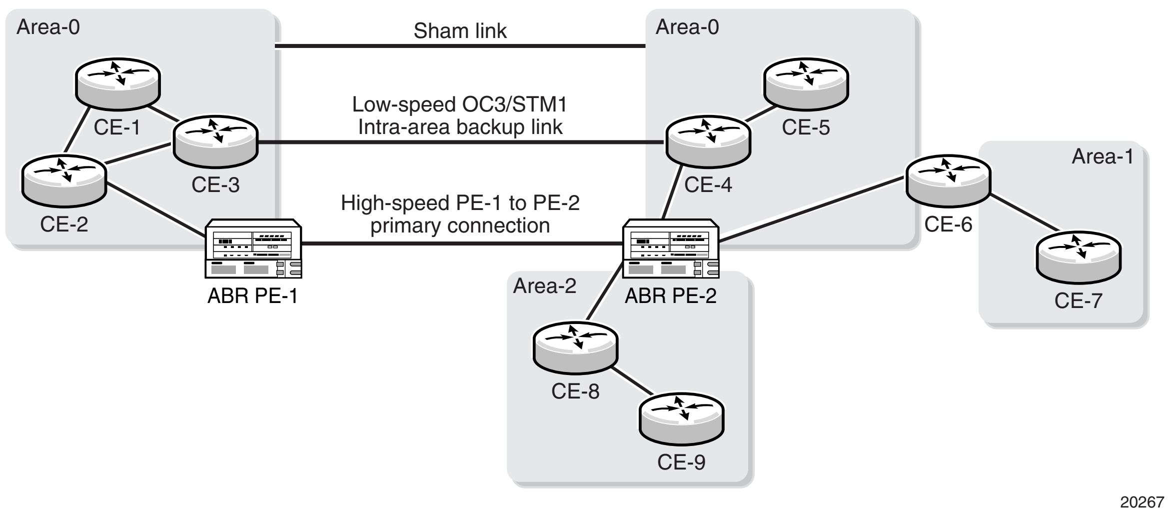
The PE router stops sending the MDT join TLV when the transmission bandwidth no longer exceeds the configured threshold. The PE routers using the data-MDT leave the group and transmission resumes over the default MDT.

OSPF sham link support

You can use the OSPF protocol to connect CE routers to PE routers over an MPLS VPN backbone. This can be useful for customers who subscribe to a VPN service and want to use OSPF as their intra-site routing protocol to exchange routing information between their sites. However, there is a potential configuration issue associated with this approach.

OSPF PE-CE connections assume that the only path between two client sites is across the MPLS VPN backbone. OSPF treats a link through a Layer 3 VPN as an inter-area link. However, other paths between VPN sites may also exist. For example, in Figure 74-1, the link between CE-3 and CE-4 (two CE routers in the same OSPF area) might be a low-speed OC3/STM1 intra-area backup link. OSPF preferentially utilizes intra-area links over inter-area links, and since it establishes an intra-area route connection between CE-3 and CE-4, the potentially high-speed PE-1 to PE-2 primary connection is not utilized.

Figure 74-1 Sham link configuration example



OSPF sham links can be created to resolve this problem. By creating and configuring a sham link as an intra-area link between PE-1 and PE-2, a normal OSPF adjacency is formed, and the link-state database is exchanged across the MPLS VPN. As a result, the desired intra-area connectivity is created between PE-1 and PE-2. In addition, the cost of the CE-3/CE-4 and PE-1/PE-2 links can be managed by the use of a numerical metric. You could then configure the service so that the CE-3/CE-4 link becomes a standby link only in event that the VPN fails.

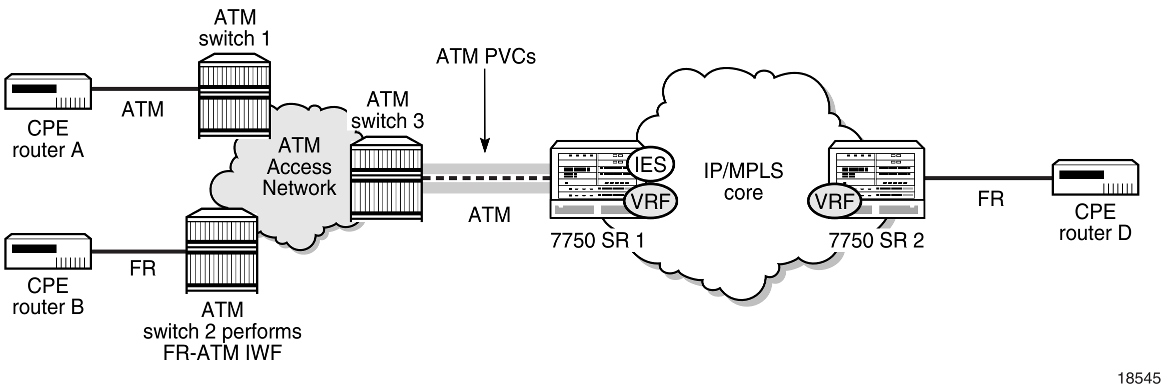
The use of OSPF sham links in the VPRN context is only applicable to 7450 ESS, 7710 SR and 7750 SR nodes.

ATM SAP terminations for VPRN

CE routers that have access to an ATM network can connect with a VPRN using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, or directly through ATM connections.

Figure 74-2 shows how CPE Router A in an ATM network can access L3 IP services, such as a VPRN, using a statically configured ATM PVC on a 7750 SR (SR#1). A SAP is configured on SR #1 to serve a specific VPRN as identified by the VRF. Destination CPE router D can receive RFC 2684-encapsulated traffic over an IP network through a Frame Relay over 7750 SR 2.

Figure 74-2 ATM SAP network connection to a VPRN



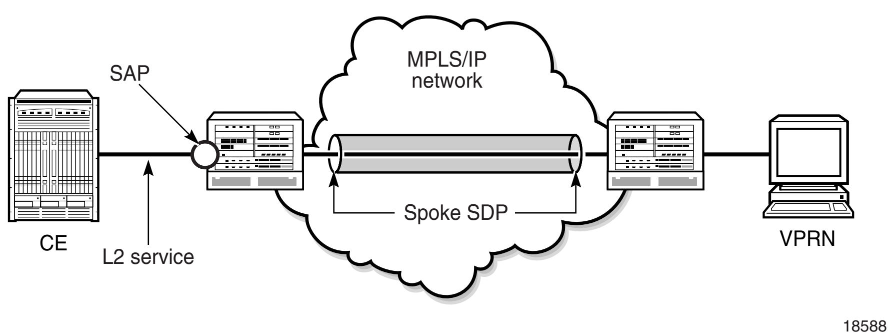
The two connection methods used between ATM and VPRN, which appear in 5620 SAM as AAL5 Encapsulation parameters: LLC/SNAP encapsulation and VC-multiplexing.

Epipe SDP spoke termination on VPRN services

A VLL Epipe service can terminate directly on a VPRN service using an SDP spoke on the 7750 SR, 7450 ESS, or 7710 SR. Traffic that terminates on a VPRN service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by VPRN are also supported for spoke SDP termination.

Figure 74-3 shows a spoke SDP terminating directly on a VPRN. The spoke SDP could be tied to an Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 74-3 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID, which must be unique within the NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for each SRRP instance associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism that controls state transitions is based on a dynamic priority level that an SRRP instance maintains. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

To prevent a flood of AccessInterfaceDown alarms that an SRRP fault or link failure may generate for LAG-based MSAPs, the 5620 SAM performs alarm suppression. See chapter 68 for more information.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

The 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12 support DoS protection policies.

To protect a VPRN from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPRN L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPRN L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPRN L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 21-3 for information about creating a DoS protection policy.

Local DHCP servers

The 5620 SAM supports configuring local DHCP servers on the 7710 SR and 7750 SR, and on the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the Local DHCP server.

- Subscriber aggregation in a single node or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

Local user database

The 5620 SAM supports the configuration of a local user database on the 7710 SR and 7750 SR, and on the 7450 ESS. The local database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured, otherwise it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. After a local user database is configured, it can be associated with a local DHCP server and PPPoE configurations on group interfaces.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address are not authenticated.

PPPoE protocol on VPRN services

A VPRN service can be configured to run PPPoE protocol. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. From the group interface configuration form you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

PPPoE termination in a business VPRN environment is also supported. This ability targets applications such as PPPoE VPRN with IP overlap, where there are two participants in the service:

- The “Wholesale VPRN”, which is a VPRN that provides access to the SAP.
- The “Retail VPRN”, which is a business VPRN that routes the packets belonging to the PPPoE sessions terminating in it. The Retail VPRNs may have overlapping IP addresses.

In this configuration, the PPPoE subscriber host terminates in a Retail VPRN and provides a routed path to the customer site. The VPRN service-id that carries it is determined by the service configuration, specifically:

- If a local user database is used, the Retail Service ID property that you specify in the PPPoE host configuration provides a reference to the VPRN service-id that should be used.
- If RADIUS is used for authentication, the retailer service-id is provided by an Alcatel-Lucent VSA.
- If MSAP is used, the SAP is created in the wholesale VPRN using the information from RADIUS.

The PPPoE session is negotiated with the parameters defined by the Wholesale VPRN interface. Since the IP address space of the subscriber management host may overlap between VPRN services, the node anti-spoofs the packets at access ingress with the session-id.

L2TP on VPRN services

The 5620 SAM supports the configuration of L2TP on a Release 8.0 or later 7710 SR or 7750 SR, and on the 7450 ESS in mixed mode. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

Note — On a Release 7.0 7750 SR that acts as an LAC NE, each L2TP tunnel must have the local IP address set to the system interface IP address.

See chapter 18 for more information about ISA-LNS groups. See Procedure 18-7 for information about how to create and configure an ISA-LNS group. See chapter 31 for more information about L2TP.

See Procedure 74-1 for information about enabling L2TP on a VPRN router instance site. See Procedure 74-13 for information about configuring a VPRN group interface to terminate LNS PPP sessions.

IPsec

You can configure a VPRN with a tunnel interface for secure and encrypted tunneling between sites. An IPsec VPRN allows you to share secure and encrypted VPN traffic among multiple sites.

IPsec VPRN services include:

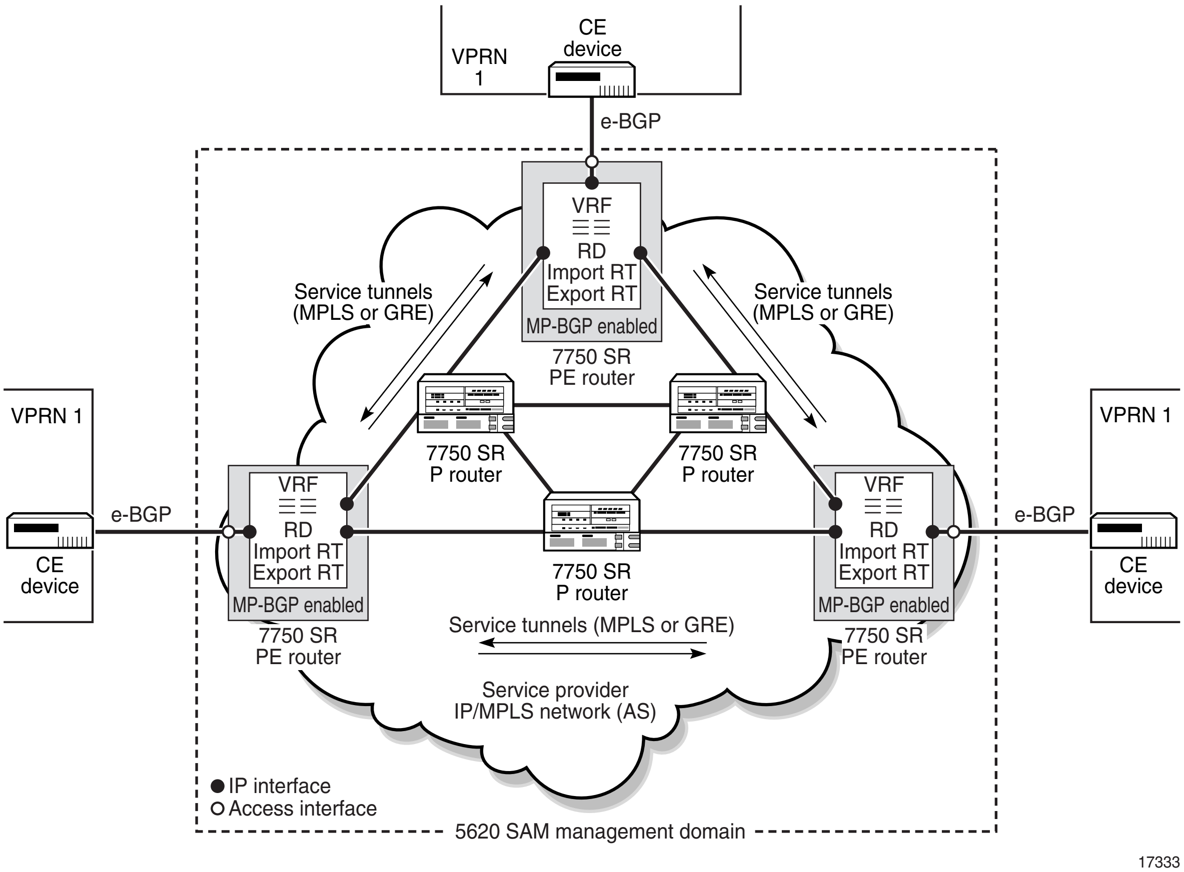
- NAT traversal
- DES, 3DES, AES-128, AES-192 and AES-256 encryption methods
- HMAC-MD5 and HMAC-SHA1 authentication and hashing methods
- Diffie-Hellman key generation algorithms
- Pre-shared keys and IKE shared secret with PFS key management authentication methods

See chapter 35 for more information about IPsec configuration.

74.2 Sample VPRN service configuration

Figure 74-4 shows a sample VPRN service configuration.

Figure 74-4 Sample VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 74-2 lists the high-level tasks that are required to configure the sample VPRN service.

Table 74-2 Sample VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.

2. Configure ports as access ports for use in the service	Right-click on a port from the equipment navigation tree and choose Properties. Specify the port as an access port and optionally specify an encapsulation type.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 31 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Protocols tab and select the BGP check mark box. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1.	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 9 for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the VPRN service sites. Perform the following for each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 31 for information about routing protocol configuration.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure an access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign an AA transit IP or transit prefix policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

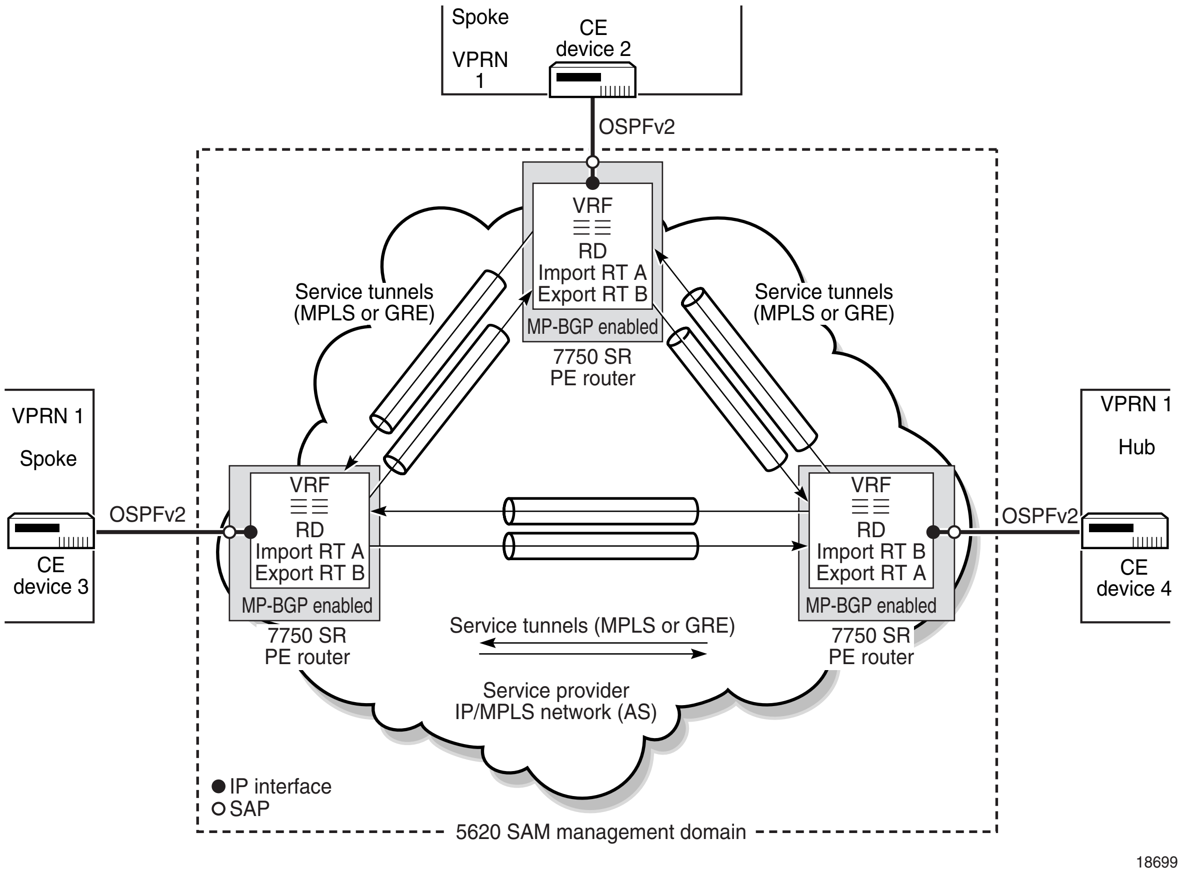
(2 of 2)

74.3 Sample hub-and-spoke VPRN configuration

In a hub-and-spoke VPRN, the majority of the traffic is exchanged between the hub (for example, headquarters) and spoke sites (for example, branches). Traffic between spoke sites passes through the hub site. Spoke sites advertise their routes to the hub site, which in turn advertises these routes to the other spoke sites.

Figure 74-5 shows a sample hub-and-spoke VPRN service configuration. Your configuration will vary depending on your network requirements.

Figure 74-5 Sample hub-and-spoke VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 74-3 lists the high-level tasks that are required to configure this sample hub-and-spoke VPRN service.

Table 74-3 Sample hub-and-spoke VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
	• DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form.

2. Configure ports as access ports for use in the service	Right-click on a port in the equipment navigation tree and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 31 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Protocols tab and select the BGP check mark box. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 9 for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the sites for VPRN 1. For each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 31 for information about routing protocol configuration.
	  • Configure other routing protocols on the sites, as required.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups. See chapter 31 for more information about protocol configuration.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure one or more access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Assign an application profile, if required.
	  • Assign an AA transit IP or transit IP policy, if required.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

(2 of 2)

74.4 Workflow to create a VPRN service

The following workflow lists the high-level steps required to create a VPRN service. As a prerequisite for creating a VPRN service, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.

- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1 for more information.
- the access ports for the service are created; see chapter 20 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.
- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.

1 Create the VPRN service. See Procedure 74-1 for more information.

i Choose a customer to associate with the VPRN service

ii Define the general properties for the VPRN service.

iii Configure NAT on the VPRN Site.

iv Configure multicasting for the VPRN service, if required.

v Enable one or more routing protocols on the VPRN site.

vi Configure a GSMP group on the site, if required.

vii Configure a local DHCP server or DHCP v6 server on the routing instance, if required.

viii Turn up the VPRN service.

2 Perform one or more of the following, as required.

a create an L3 access interface for the VPRN site; see Procedure 74-2 for more information

b create an L3 network interface for the VPRN site; see Procedure 74-3 for more information

c add a GNE site and GNE service interfaces to an existing VPRN service; see Procedure 74-4 for more information

d configure BGP, OSPFv2, OSPFv3, PIM, IGMP, RIP or L2TP in the VPRN routing instance; see Procedure 74-5 for more information

e configure IGMP on a VPRN routing instance; see Procedure 74-6 for more information

f add a Global Route Table to a VPRN site; see Procedure 74-7 for more information

g add a PIM interface to the VPRN; see Procedure 74-8 for more information

h add an IGMP interface to the VPRN; see Procedure 74-9 for more information

i create a VPRN spoke SDP binding; see Procedure 74-10 for more information

- **j** create an L2 SDP spoke termination on a VPRN service; see Procedure 74-11 for more information
- **k** add a subscriber interface to the VPRN; see Procedure 74-12 for more information
- **l** add a group interface to the VPRN (only the 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in a VPRN); see Procedure 74-13 for more information
- **m** collect and view PPP ATM SAP statistics and information for a VPRN group interface; see Procedure 74-14 for more information
- **n** add an IP mirror interface to the VPRN; see Procedure 74-15 for more information
- **o** to implement dual homing using SRRP; see Procedure 74-16 for more information
- **p** create an intra-area OSPF sham link between two VPRN sites; see Procedure 74-17 for more information
- **q** add a tunnel interface to a VPRN; see Procedure 35-6 for more information
- **r** Create and enable a video interface for the VPRN, if required. See Procedure See Procedure 36-1 for more information.

3 As required, run an OAM validation test for a VPRN. See Procedure 74-18 for more information.

4 As required, view VPRN service information:

- **a** view the service topology map associated with a VPRN service; see Procedure 74-19 for more information
- **b** view the VPRN service operational status; see Procedure 74-20 for more information
- **c** view the DHCPv6 prefixes that the server has given out; see Procedure 74-21 for more information
- **d** view the lease not owner and pool unknown log events for local DHCPv6 servers; see Procedure 74-22 for more information

5 As required, modify a VPRN service:

- **a** using the Manage Services form; see Procedure 74-23 for more information
- **b** using the topology view; see Procedure 74-24 for more information

6 As required, delete a VPRN service. See Procedure 74-25 for more information.

74.5 VPRN service management procedures

Use the following procedures to perform VPRN creation and management tasks.

Procedure 74-1 To create a VPRN service

1 Choose Create→Service→VPRN from the 5620 SAM main menu. The VPRN Services (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPRN. The Select Customer - VPRN Service form opens.

3 Select a customer for the VPRN and click on the OK button. The Select Customer - VPRN Service form closes and the VPRN Services (Create) form refreshes with the customer information.

4 Configure the parameters:

- Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Auto-Assign ID
- SVC Mgr Service ID
  This parameter is configurable when the Auto-Assign ID parameter is disabled.
- Service Name
- Description
- Service Tier
- Service Prioirity
- Administrative State
- Automatic SDP Binding Creation
- IP Address Overlap Avoidance Enabled
- Profile Name
  This parameter is configurable when the Automatic SDP Binding Creation parameter is enabled.
- OLC State
  This parameter is configurable when you click on the Apply button on the VPRN Service (Create) form.

5 To configure parameters for AA reporting to the 5670 RAM, perform the following steps.

i Click on the 5670 RAM Parameters tab button.

ii Click on the General tab button.

iii Configure the parameters:

- Enable Application Performance Reporting
- Report Customer Name

6 Perform one of the following:

a Create a site for the VPRN. Go to step 7.

b Complete service creation, if sites and access interfaces for the VPRN are to be created later. Go to step 82.

For information on adding a GNE site to a VPRN service, see Procedure 74-4.

7 On the navigation tree, right-click on the Site icon and choose Create VPRN Site. The Select Network Elements - VPRN Service form opens with a list of available sites displayed.

8 Select a site and click on the OK button. The VPRN Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Enable Hash Label
- GSMP Administrative State
- Tunnel Fault Notification

Tunnel Fault Notification is configurable on sites where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

10 To configure NAT on the VPRN Site, click on the NAT Configuration tab button. Otherwise, go to step 23.

Note — NAT configuration is supported only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher.

11 Click on the Create button. The NAT Configuration (Create) form opens with the General tab displayed.

12 Click on the Select button to choose a NAT policy. The Select NAT policy form opens.

13 Select a policy in the list and click on the OK button. The Select NAT policy form closes, and the policy name is displayed on the NAT Configuration (Create) form.

14 Click on the Apply button. A dialog box appears.

15 Click on the Yes button.

16 Perform the following steps to configure static port forwarding, if required.

Note — You can configure NAT static port forwarding only for large-scale NAT.

i Click on the NAT Static Port Forwarding tab button.

ii Click on the Create button. The NAT Static Port Forwarding Display (Create) form opens.

iii Configure the parameters:

- Inside IP Address
- Outside IP Address
- Inside Port
- Protocol
- Outside Port
- Lifetime (seconds)

Note — You cannot specify the same set of Inside Port and Protocol values in more than one static port mapping to an Inside IP Address.

You can specify the same Outside Port value in multiple mappings to an Inside IP Address.

iv Click on the OK button. The NAT Static Port Forwarding (Create) form closes, and the new entry is listed on the NAT Configuration form.

17 Perform the following steps to synchronize NAT static port forwards, if required.

i Choose a static port forward from the list and click on the Sync button. The NAT Static Port Forwarding Sync form opens.

ii Click on the Select button in the Targeted Router Instance panel. The Select Targeted Router Instance form opens.

iii Select a router instance from the list and click on the OK button. The Select Targeted Router Instance form closes and the NAT Static Port Forwarding Sync form reappears with the router instance information displayed.

iv Configure the Lifetime (seconds) parameter and click on the OK button. A dialog box appears.

v Click on the OK button.

18 Perform the following steps to configure a NAT pool.

i Click on the NAT Pools tab button.

ii Click on the Create button. The NAT Pool (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Description
- NAT Pool Type
- Administrative State
- Port Reservation Type
- Port Reservation Value
- Port Forward Range End
- High Watermark
- Low Watermark

iv Click on the Select button to choose an ISA-NAT group. The Select ISA-NAT group form opens.

- **v** Select an ISA-NAT group in the list and click on the OK button. The Select ISA-NAT group form closes, and the ISA-NAT group name is displayed on the NAT Pool (Create) form.
- **vi** Click on the NAT Pool Ranges tab button.
- **vii** Click on the Create button. The NAT Pool Range (Create) form opens.
- **viii** Configure the parameters:
    - Description
    - Range Start
    - Range End
- **ix** Click on the OK button. A dialog box appears.
- **x** Click on the OK button. The NAT Pool Range (Create) form closes, and the NAT Pool (Create) form lists the pool range.
- **xi** Click on the OK button. A dialog box appears.
- **xii** Click on the OK button. The NAT Pool (Create) form closes, and the NAT Configuration (Create) form lists the NAT pool.
- **xiii** Repeat steps vii to xii to add another pool, if required.

19 Perform the following steps to add an IP address for L2-aware NAT forwarding, if required.

- **i** Click on the L2 Aware IP Addresses tab button.
- **ii** Click on the Create button. The L2 Aware IP (Create) form opens.
- **iii** Configure the parameters:
    - Inside IP Address
    - Prefix Length
- **iv** Click on the OK button. A dialog box appears.
- **v** Click on the OK button. The L2 Aware IP (Create) form closes, and the NAT Configuration (Create) form lists the IP address.
- **vi** Repeat steps ii to v to add another IP address, if required.

20 Perform the following steps to add a NAT destination address.

- **i** Click on the NAT Destinations tab button.
- **ii** Click on the Create button. The NAT Destination (Create) form opens.
- **iii** Configure the parameters:
    - Inside IP Address
    - Prefix Length
- **iv** Click on the OK button. A dialog box appears.

v Click on the OK button. The NAT Destination (Create) form closes, and the NAT Configuration (Create) form lists the destination.

vi Repeat steps ii to v to add another destination, if required.

21 Click on the OK button. A dialog box appears.

22 Click on the Yes button. The NAT Configuration (Create) form closes, and the NAT configuration is listed on the VPRN Site form.

23 If the VPRN site is to support multicasting, click on the MVPN tab button and perform steps 24 to 34; otherwise go to step 35.

24 Click on the Routing sub-tab to configure an MVPN VRF instance.

25 Configure the MVPN VRF Target Type parameter:

Note 1 — Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

Note 2 — A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

a Specify None if you do not want to specify a VRF target for the site. Go to step 29.

b Specify Define Default if you want to specify a default VRF target for the site. Go to step 26.

c Specify Define Import and Export if you want to specify import and export VRF targets for the service site. Go to step 27.

26 Configure the Target Format parameter by performing one of the following steps:

a To specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

The Target AS Value is the Autonomous System number of the PE node. For the Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 45.

c To specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

27 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 28.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

The Import Target AS Value is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 28.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 28.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 28.

28 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 29.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 29.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 29.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) parameter is the four-byte Autonomous System number of the PE node. For the Export Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 29.

29 Click on the Import Policies sub-tab.

30 Configure the Import Unicast parameter. If you set the parameter to True, go to step 32.

31 Specify up to five Unicast import policies by using the Select button to choose a policy from the filtered list.

32 Click on the Export Policies sub-tab.

33 Configure the Export Unicast parameter. If you set the parameter to True, go to step 35.

34 Specify up to five VRF export policies by using the Select button to choose a policy from the filtered list.

35 If the VPRN site is to support IPv6 addressing (for router advertisement or neighbor discovery) or VRRP objects, perform the following sub steps to configure an SNMP community for mediating the IPv6 objects.

i Click on the SNMP Community tab button.

ii Click on the Create button. The SNMP Community (Create) form opens.

iii Configure the SNMP Community String parameter.

iv Click on the OK button. The SNMP community string entry is displayed on the Site (Create) form and a dialog box appears.

v Click on the OK button. The SNMP Community (Create) form closes.

Note — When the 5620 SAM uses SNMPv2 for device mediation, you must configure one and only one SNMP community string for the VPRN site. Otherwise, there is no mediation of the VPRN IPv6 objects on the site, and the 5620 SAM raises an alarm. The alarm is cleared and mediation resumes after the configuration is modified so that exactly one SNMP community string is associated with the VPRN site.

36 Perform the following sub stages to enable one or more routing protocols on the VPRN site.

i Click on the Protocols tab button.

ii Configure the parameters:

- BGP Enabled
- OSPFv2 Enabled
- OSPFv3 Enabled
- RIP Enabled
- L2TP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.

iii If both the OSPFv2 Enabled parameter and the OSPFv3 Enabled parameter are disabled, navigate to the Components view of the VPRN, right-click on Protocols, then select Create OSPF. The OSPF Routing Instance (Create) form opens. In the OSPF Instance panel, configure the Version parameter.

iv Configure multicast for the site, if required. Click on the Multicast tab button.

v Configure the parameters:

- PIM Enabled
- IGMP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.

37 Click on the Routing tab button to configure a routing instance. The General tab is displayed.

38 Configure the parameters:

- Router ID
- Maximum Number Of Equal Cost Routes
- Autonomous System
- FIB Priority
- Type
- Label Mode
- Carrier Carrier VPN
- Route Distinguisher Type
- Enforce Maximum Number Of Routes
- Enforce Maximum Number Of Multicast Routes
- Maximum Number Of IPv6 Routes
- Log Only
- Threshold (%)

You cannot configure the Carrier Carrier VPN parameter on a VPRN site if there are any pre-existing interfaces configured on the site.

When you set the Route Distinguisher Type parameter to Type 0, the following configurable parameters appear:

- Type 0 Administrative Value
- Type 0 Assigned Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique RD from the drop-down menu.

The Type 0 Administrative Value is the Autonomous System (AS) number of the PE node. For the Type 0 Assigned Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

When you set the Route Distinguisher Type parameter to Type 1, the following configurable parameters appear:

- Type 1 IP Address
- Type 1 Assigned Value

When you set the Route Distinguisher Type parameter to Type 2, the following configurable parameters appear:

- Type 2 Administrative Value
- Type 2 Assigned Value

When you select the Enforce Maximum Number Of Routes parameter, the following configurable parameters appear:

- Maximum Number Of Routes
- Log Only
- Threshold (%)

When you select the Enforce Maximum Number Of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number Of Multicast Routes
- Log Only
- Threshold (%)

39 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

40 Click on the VRF Target tab button to configure a VRF instance.

41 Configure the VRF Target Type parameter:

Note 1 — Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

Note 2 — A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

a Specify None if you do not want to specify a VRF target for the site. Go to step 45.

b Specify Define Default if you want to specify a default VRF target for the site. Go to step 42.

c Specify Define Import and Export if you want to specify import and export VRF targets for the service site. Go to step 43.

42 Configure the Target Format parameter by performing one of the following steps:

a To specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value is the Autonomous System number of the PE node. For the Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 45.

c To specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

43 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 44.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 44.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

44 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 45.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 45.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Export Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 45.

45 Configure ingress multicast forwarding, if required.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button beside the Name parameter. The Select Ingress Info Policy - Service L3 Routing list form opens.

iii Choose an ingress info policy and click on the OK button. The Select Ingress Info Policy - Service L3 Routing list form closes.

Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 46 for a listing of the displayed operational channel parameters.

46 Click on the Auto-Bind tab button to configure the binding of the site to service tunnels.

47 Configure the Transport parameter.

a Choose None to explicitly specify service tunnels and circuits for the service.

b Choose LDP for the service to be automatically bound to MPLS service tunnels utilizing LDP.

Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 33-1 for more information.

c Choose RSVP-LSP for the service to be automatically bound to MPLS service tunnels utilizing RSVP-LSP.

Note — The RSVP-LSP option is available only on the 7450 ESS in mixed mode, the 7710 SR, and 7750 SR.

d Choose RSVP or LDP for the service to be bound to MPLS service tunnels utilizing either RSVP or LDP.

This choice provides the ability to simultaneously support both tunnel options, in networks that have a mixture of LDP and RSVP-TE in place. 5620 SAM always tries to resolve the VPN route by using RSVP-LSP tunnels first (lowest metric). If no RSVP-LSP service tunnels are available, then tunnels configured for LDP are used. If RSVP-LSP tunnels subsequently become available again, then the route resolution automatically returns to RSVP-LSP.

Note — The RSVP or LDP option is available only on the a 7450 ESS in mixed mode, and on the Release 7.0 R3 or later 7710 SR and 7750 SR.

e Choose GRE for the service to be automatically bound to GRE service tunnels.

48 Click on the VRF Import Policies tab button.

49 Specify up to five VRF import policies by using the Select button to choose a policy from the filtered list.

50 Click on the VRF Export Policies tab button.

51 Specify up to five VRF export policies by using the Select button to choose a policy from the filtered list.

52 Configure static routes, if required.

i Click on the Static Routes tab button.

ii Click on the Create button to define a static route that the PE VRF is to exchange with the CE. The Static Route (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Forwarding Class Name
- Forwarding Class Priority
- Multicast Capable Peers
- Destination
- Prefix Length
- Type
- IP Address
- Preference
- Metric
- Administrative State
- Tag
- Enable CPE Check
- Target IP Address
- Target IP Address
- Drop Count
- Log
- Prefix List Name
- Prefix List Flag

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are only displayed when Enable CPE Check is enabled.

You cannot specify a Prefix List if either BFD Enabled or Enable CPE Check parameters are enabled for the static route.

The Prefix List Flag Prefix List Name parameter is configured.

iv Click on the OK button. The Static Route (Create) form closes and the Site (Create) form reappears.

53 Configure a GSMP group on the site, if required.

i Click on the GSMP tab button.

ii Click on the Create button. The GSMP Group (Create) form opens with the General tab displayed.

iii Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- OAM Administrative State
- Dynamic Topology Discovery

iv Click on the GSMP Group Neighbor tab button.

v Click on the Create button. The GSMP (Create) form opens with the General tab displayed.

vi Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

vii Click on OK button. The GSMP (Create) form closes.

viii Click on OK button. The GSMP Group (Create) form closes.

54 Click on the Local DHCP Servers tab button and perform one of the following steps to configure a local DHCP server on the routing instance, if required or applicable.

Note — DHCPv6 server configuration is supported only on a Release 9.0 R1 or later 7750 SR or 7450 ESS in mixed mode.

a To configure a local DHCPv4 server on the routing instance go to step 55.

b To configure a local DHCPv6 server on the routing instance go to step 56.

55 Perform the following steps to configure a local DHCPv4 server on the VPRN routing instance, if required.

i Click on the Local DHCP V4 tab button.

ii Click on the Create button. The Local DHCP Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use GI Address

iv Click on the Select button. The Select Local User Database form opens.

v Select a local user database in the list and click on the OK button. The Select Local User Database form closes and the local user database information is displayed on the Local DHCP Servers (Create) form.

vi Configure the following parameters:

- Allow Send Force Renews
- Use Pool From Client

vii Click on the IP Address Pools tab button to assign one or more IP addresses to the local DHCP server.

viii Click on the Create button. The IP Address Pool (Create) form opens with the General tab displayed.

ix Configure the following parameters:

- Pool Name
- Description

x Configure the parameters in the Minimum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xi Configure the parameters in the Maximum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Offer Time panel:

- Minutes
- Seconds

xiii Configure the parameters in the Pool Minimum Free panel:

- Type
- Threshold

xiv Click on the Subnets tab button to add subnets to the DHCP server pool.

xv Click on the Create button. The Subnet (Create) form opens with the General tab displayed.

xvi Configure the parameters:

- IP Address
- Prefix Length
- Free Addresses Minimum Type
- Free Addresses Minimum Threshold
- Maximum Declined Addresses Stored

xvii Click on the Address Ranges tab button.

xviii Click on the Create button. The Subnet Address Range (Create) form opens.

xix Configure the parameters:

- Action
- Start Address
- End Address

Note — You must exclude static IP addresses from the subnet address range because static IP addresses are dedicated.

xx Click on the OK button. The Subnet Address Range (Create) form closes and a dialog box appears.

xxi Click on the OK button. The Subnet (Create) form reappears.

xxii Click on the Options tab button.

xxiii Click on the Create button. The Subnet Option (Create) form opens.

xxiv Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxv Click on the OK button. The Subnet Option (Create) form closes and a dialog box appears.

xxvi Click on the OK button. The Subnet (Create) form reappears.

xxvii Click on the OK button. The Subnet (Create) form closes and a dialog box appears.

xxviii Click on the OK button. The IP Address Pool (Create) form reappears.

xxix Click on the Options tab button.

xxx Click on the Create button. The IP Address Pool Option (Create) form opens.

xxxi Configure the Option parameter.

xxxii If you set the Option parameter to Custom Option, configure the following parameters:

- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxxiii If you set the Option parameter to DNS Name Servers or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

xxxiv If you set the Option parameter to Domain Name, configure the Value parameter.

xxxv If you set the Option parameter to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

xxxvi If you set the Option parameter to Netbios Node Type, configure the Netbios Node Type parameter.

xxxvii Click on the OK button. The IP Address Pool Option (Create) form closes and a dialog box appears.

xxxviii Click on the OK button. The IP Address Pool (Create) form reappears.

xxxix Click on the OK button. The IP Address Pool (Create) form closes and a dialog box appears.

xl Click on the OK button. The Local DHCP Server (Create) form reappears.

xli Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

xlii Click on the OK button. The VPRN Site (Create) form reappears.

56 Perform the following steps to configure a local DHCP v6 server on the routing instance, if required or applicable.

Note — DHCPv6 server configuration is supported only on a Release 9.0 R1 or later 7750 SR or 7450 ESS in mixed mode.

i Click on the DHCP V6 tab button.

ii Click on the Create button. The Local DHCPv6 Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use Pool From Client

iv Configure the parameters in the Lease Hold Time panel:

- Days
- Hours
- Minutes
- Seconds

v Click on the IPv6 Address Pools tab button to assign one or more pools to the local DHCPv6 server.

vi Click on the Create button. The IPv6 Address Pool (Create) form opens with the General tab displayed.

vii Configure the following parameters:

- Pool Name
- Description

viii Click on the Prefixes tab button to add prefixes to the DHCPv6 server pool.

ix Click on the Create button. The Prefix (Create) form appears with the General tab displayed.

x Configure the following parameters:

- IPv6 Address
- Prefix Length

xi Configure the parameters in the Preferred Life Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Valid Life Time panel:

- Days
- Hours
- Minutes
- Seconds

xiii Configure the parameters in the Renew Timer panel:

- Days
- Hours
- Minutes
- Seconds

xiv Configure the parameters in the Rebind Timer panel:

- Days
- Hours
- Minutes
- Seconds

xv Click on the Apply button. A dialog box appears.

xvi Click on the OK button.

xvii Click on the Options tab button.

xviii Click on the Create button. The Prefix Option (Create) form appears.

xix Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xx Click on the OK button. The Prefix Option (Create) form closes and a dialog box appears.

xxi Click on the OK button. The Prefix (Create) form reappears with Options tab displayed.

xxii Click on the OK button. The Prefix (Create) form closes and a dialog box appears.

xxiii Click on the OK button. The IPv6 Address Pool (Create) form reappears with Prefix tab displayed.

xxiv Click on the Options tab button.

xxv Click on the Create button. The IPv6 Address Pool Option (Create) form appears.

xxvi Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String or Domain.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxvii Click on the OK button. The IPv6 Address Pool Option (Create) form closes and a dialog box appears.

xxviii Click on the OK button. The IPv6 Address Pool (Create) form reappears with Options tab displayed.

xxix Click on the OK button. The IPv6 Address Pool (Create) form closes and a dialog box appears.

xxx Click on the OK button. The DHCP V6 Server (Create) form reappears with IPv6 Address Pool tab displayed.

xxxi Click on the OK button. The DHCP V6 Server (Create) form closes and a dialog box appears.

xxxii Click on the OK button. The VPRN Site (Create) form reappears.

57 Click on the Self Generated Traffic tab button. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

58 Choose an application to view or edit the DSCP setting.

59 Click on the Properties button. An Application DCSP Marking form opens.

60 Configure the DSCP parameter.

61 Click on the Apply button. A dialog box appears. Click on the OK button.

62 Click on the DSCP Mapping tab. A list of DSCP types and corresponding forwarding classes is displayed.

63 Choose a DSCP to view or edit the forwarding class.

64 Click on the Properties button. An Application DCSP Marking form opens.

65 Configure the Forwarding Class parameter.

66 Click on the Apply button. A dialog box appears. Click on the OK button.

67 Click on the Dot1p Marking tab button. A list of applications for which the Dot1p can be set is displayed.

68 Choose a Dot1p to view or edit the setting.

69 Click on the Properties button. An Application Dot1p Marking form opens.

70 Configure the dot1p parameter.

71 Click on the OK button. A dialog box appears. Click on the OK button.

72 Configure an override source IP address or L3 interface for use by a selected IP application, if required.

  i Click on the Source Addresses tab button.

  ii Click on the Create button. The Source Address (Create) form opens.

73 Choose an IP application from the Source IP Application drop-down menu.

74 Specify the source address for the IP application server by performing one of the following steps:

Note — If you choose the interface index option, the router used for this VPRN must already have an access interface created for its routing instance.

a Choose IP Address in Source Address Termination to specify the source IP address of the IP application server.

i Enter a valid IP address that the VPRN virtual routing instance will identify in the Source IP Address field.

ii Go to step 75.

Note 1 — An IPv6 address option for the Source IP Address parameter is available when the IPv6 Allowed parameter is set during network interface creation. See chapter 30 for more information about creating a network interface.

Note 2 — You must select an IPv6 Source IP Address before you can select IPv6 Source IP Applications.

b Choose Interface Index in Source Address Termination to use the primary address of the L3 network interface as the source address of the IP application server.

i Click on the Select button to choose an interface. The Select Source Address VPRN Interface - Source Address form opens. Choose an interface from the list and click on the OK button. The IP address and Interface ID of the L3 interface appear on the form.

ii Go to step 75.

75 Click on the OK button. The Source Address (Create) form closes and the Site (Create) form reappears. The IP application source address and parameters appear on the form.

76 Click on the IGMP Host Tracking tab button.

77 Configure the parameters:

- Expiry Time
- Administrative State

78 Click on the Route Aggregation tab button to configure route aggregates for the VPRN service.

Route aggregation allows you to group a number of routes with common IP prefixes into a single entry in the routing table. This reduces the number of routes that need to be advertised by the hosting router and reduces the number of routes in the routing tables of downstream routers.

Note — Route aggregation for VPRN sites is supported on 7450 ESS in mixed mode, 7750 SR and 7710 SR nodes.

i Click on the Create button. The Aggregation (Create) form opens.

ii Configure the parameters:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Aggregator AS
- Aggregator IP Address

The IP Address Prefix you enter must be an IPv4 address in the form x.x.x.0, where the last integer is the host bits and must have a value of 0.

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True.

79 Click on the OK button. A dialog box appears.

80 Click on the OK button. The Site (Create) form closes, and the VPRN (Create) form reappears with the new site information displayed in the service navigation tree.

81 Perform one of the following:

a Create an additional site for the VPRN. Go to step 7.

b Go to step 82.

82 Click on the OK button. A dialog box appears.

83 Click on the Yes button to confirm the action. The VPRN (Create) form closes.

Procedure 74-2 To create a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, click on the site to which you want to add the access interface; expand the entries for that site.

For information on adding a GNE service interface to a VPRN service, see Procedure 74-4.

6 Right-click on Access Interfaces and choose Create L3 Access Interface. The L3 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Trusted
- Class
- IPv6 Allowed
- Admin Link Local Address
- Admin Link Local Address Preferred
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6
- Calling Station ID
- Configured IP MTU (Octets)
- Unnumbered Type
- IP Address
- Interface Name
- URPF Check State
- URPF Check Mode
- Tunnel Fault Notification

The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

8 If the Loopback Enabled parameter in step 7 is enabled, you cannot associate a port with the L3 interface. Go to step 18.

9 Perform the following steps to bind an application profile to the VPRN L3 access interface, if required:

i Click on the Select button beside the Application Profile parameter in the Application Assurance panel. The Application Profile String: - VPRN L3 Access Interface list form opens.

ii Select a profile from the list and click on the OK button. The Application Profile String - VPRN L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.

Note — The Application Profile String: - VPRN L3 Access Interface list form only displays local profiles that already exist on the NE.

10 Choose one of the following AA transit policy types, if required.

Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — To bind a transit policy to an L3 access interface, a port must already exist on the interface.

Note 3 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 4 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Select a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

11 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab button.

12 Configure the Unicast RPF parameters, if required.

- URPF Check State
- URPF Check Mode

Note — The URPF Check State parameter must be enabled to display the URPF Check Mode parameter.

13 Click on the Port tab button.

14 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

15 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

16 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

17 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle is selected in step 15, only the Scheduling Class parameter is configurable.

18 Assign ingress and egress QoS policies to the interface, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service navigation tree, choosing Properties, and configuring the parameters on the appropriate tab.

i Click on the QoS tab button.

Note — The QoS tab is configurable only if a port is assigned to the interface.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID
- Use Multipoint Shared Queue

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is BCP dot1q, dot1q, or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L3 Access Interface form opens.

iv Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 15 has the access ingress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L3 Access Interface form opens.

vi Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress QoS policy information displayed.

Note 1 — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 15 has the access egress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

Note 2 — Queue Group Template policies are not applicable to L3 interfaces associated with HSMDA ports.

vii If you are configuring an L3 access interface for a 7710 SR or 7705 SAR, or if the port you selected in step 15 is not an HSMDA port, then go to step 19.

viii Configure the Packet Byte Offset (bytes) parameter, if required. You must enable the associated Override check box if you need to configure this parameter.

ix Click on the Select button in the Egress HSMDA Override panel to choose a WRR policy. The Select WRR Policy form opens.

x Choose a WRR policy and click on the OK button. The Select WRR Policy form closes and the VPRN L3 Access Interface (Create) form reappears with the WRR policy information displayed.

xi Click on the Select button in the Egress HSMDA Override panel to choose an HSMDA egress secondary shaper policy. The Select Secondary Shaper form opens.

xii Choose a secondary shaper and click on the OK button. The Select Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the secondary shaper information displayed.

19 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 21.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP earlier in the procedure.

20 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 15 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 15 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPRN L3 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy form opens.

vi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPRN L3 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 15 is an HSMDA port, go to step 21.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L3 Access Interface form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Policer Control Policy form closes and the VPRN L3 Access Interface (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 21.

b Specify that an aggregation scheduler policy is applied to the interface.

Note — You cannot specify an access scheduler policy if the port you selected in step 15 is an HSMDA port. Go to step 21.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L3 Access Interface form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

21 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - L3 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress IPv4 ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - L3 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress IPv4 ACL filter information displayed.

vi If the L3 Access Interface supports IPv6 addressing, perform the following substeps. Otherwise, go to step 23.

vii Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - L3 Access Interface form opens.

viii Select an ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress IPv6 ACL filter information displayed.

ix Click on the Select button in the IPv6 Egress Filter panel to choose an egress IPv6 ACL filter. The Select IPv6 Egress Filter - L3 Access Interface form opens.

x Select an egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress IPv6 ACL filter information displayed.

22 Bind a VPRN L3 access interface to a VPLS site, if required.

Note 1 — The operational state of the IP interface binding will not be turned up until the Enable IP Interface Binding parameter is set to true.

Note 2 — You can create and manage a routed VPLS connector from the navigation tree on the Composite Service (Edit) form.

i Click on the Routed VPLS tab button.

ii Enter a VPLS site name or click on the Select button next to the VPLS Name parameter to choose a VPLS site. The Routed VPLS String - VPRN L3 Access Interface form opens.

iii Select a VPLS site and click on the OK button. The VPLS site is displayed.

iv In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - VPRN L3 Access Interface form opens.

v Select an IPv4 filter and click on the OK button. The IPv4 filter information is displayed.

vi In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - VPRN L3 Access Interface form opens.

vii Select an IPv6 filter and click on the OK button. The IPv6 filter information is displayed.

viii In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - VPRN L3 Access Interface form opens.

ix Select a QoS Policy and click on the the OK button. The QoS Policy information is displayed.

23 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - L3 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

24 To associate a local DHCPv4 or DHCPv6 server to the L3 interface, if required, click on the Local DHCP tab button and perform one of the following steps.

Note — To associate local DHCPv6 servers the IPv6 Allowed parameter must be enabled.

a For local DHCPv4 servers

i Click on the Select button in the Local DHCP Server panel to choose a local DHCP server. The Select Local DHCP Server - L3 Access Interface form opens.

ii Select a local DHCP server and click on the OK button. The Select Local DHCP Server - L3 Access Interface form closes, and the L3 Access Interface (Create) form reappears with the local DHCP server information displayed.

b For local DHCPv6 servers

i Click on the Select button in the Local DHCPv6 Server panel to choose a local DHCPv6 server. The Select Local DHCPv6 Server - L3 Access Interface form opens.

ii Select a local DHCPv6 server and click on the OK button. The Select Local DHCPv6 Server - L3 Access Interface form closes, and the L3 Access Interface (Create) form reappears with the local DHCPv6 server information displayed.

Note — You cannot associate a local DHCPv4 server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up. Go to step 7 to set the Administrative State.

25 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L3 Access Interface list form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - L3 Access Interface list form closes, and the L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the interface. You must first disable the Collect Accounting Statistics parameter in step 23.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

26 Configure residential subscriber management for the interface, if required. Residential subscriber management is supported on the 7450 ESS in mixed mode, 7750 SR, and 7710 SR.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step 28.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

27 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - L3 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - L3 Access Interface form closes and the policy ID is displayed on the L3 Access Interface (Create) form.

28 Assign an IP address to the interface.

i Click on the Addresses tab button.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The L3 Access Interface (Create) form reappears with the assigned IP addresses displayed.

29 Configure IPv4 ICMP for the interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- TTL Expired
- Number of TTL Expired
- TTL Expired Time (seconds)

30 If the IPv6 Allowed parameter in step 7 is enabled, the ICMPv6 tab is configurable. Configure IPv6 ICMP, if required. Otherwise, go to step 31.

Configure the parameters:

- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- Packet Too Big
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Param Problem
- Number of Param Problem
- Param Problem Time (seconds)
- Time Exceeded
- Number of Time Exceeded
- Time Exceeded Time (seconds)

31 Configure IPCP for the interface, if required. IPCP is available only on the ASAP MDA on the 7750 SR and 7710 SR.

i Click on the IPCP tab button.

ii Configure the parameters:

- Peer Address
- Primary DNS Address
- Secondary DNS Address

Note — Primary and secondary DNS addresses have similar functionality however they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to confirm the action.

The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

32 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button.

ii Click on the Configuration tab button.

iii Configure the parameters:

- Administration Status
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier

The Transmit Interval, Receive Interval, Receive Interval, Echo Interval, and Multiplier parameters are configurable only when the Administration Status is set to Up.

iv To view local and remote session peers that are managed by the 5620 SAM. Click on the BFD Session tab button. A list of BFD current sessions on a router interface or an L3 interface appears.

v Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

vi Close the form.

Note 1 — You cannot configure BFD for an interface if BFD is disabled. See chapter 31 for information about enabling and disabling BFD for routing protocols.

Note 2 — If the IPv6 Allowed parameter in step 7 is enabled, you can configure the above BFD parameters for IPv6.

33 Configure ARP for the interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

34 If the IPv6 Allowed parameter in step 7 is enabled, the Neighbor Discovery tab is configurable. Configure neighbor discovery, if required. Otherwise, go to step 35.

i Click on the Neighbor Discovery tab button.

ii Click on the Create button. The Neighbor Discovery (Create) form opens.

iii Configure the parameters:

- IP Address
- Physical Address

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Neighbor Discovery (Create) form closes, and the L3 Access Interface (Create) form refreshes with the neighbor entry.

vi Click on the Proxy ND tab button.

vii Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 1
- Policy 1
- Policy 1
- Policy 1

Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 1 parameters and leave the Policy 1 parameter unconfigured, or the 5620 SAM reorders the policies and move the policy specified for the Policy 1 parameter to the Policy 1 parameter.

viii Repeat steps i to vii for each neighbor entry you want to create.

35 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

The Lease Populate parameter is configurable when the Enable parameter is enabled.

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step viii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

v Click on the Search button.

vi Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the L3 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source

The Remote ID String parameter is configurable when the Remote ID is set to Remote ID String.

viii Click on the Server tab button.

ix Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

36 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L3 Access Interface form reappears with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L3 Access Interface (Create) form reappears with the egress ATM policy information displayed.

37 Click on the VRRP tab button to create a VRRP instance on the current L3 interface for a virtual router. You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- Two sub-tabs are available under the VRRP tab, one for IPv4 instances and the other for IPv6 instances. You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter in step 7.
- The Link Local Address on the parent interface has to be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. To do this, the Admin Link Local Address and Admin Link Local Address Preferred parameters in step 7 must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 28 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 39 for the router advertisement on the parent interface.

See chapter 39 for configuration information about VRRP instances and virtual routers.

i Click on the Create button. The VRRP Instance (Create) form opens with the General tab displayed.

ii Configure the Virtual Router ID parameter.

iii Perform steps 8 to 15 of Procedure 39-2.

Note — You can use the VR Instances tab to create, modify, and view VR instances.

iv Click on the OK button. The VRRP Instance (Create) closes and the L3 Access Interface (Create) form reappears.

38 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Populate

The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

iii Click on the Static Hosts tab button to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management. Otherwise, go to step 39.

iv Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address

Specify at least one IP address or MAC address for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

Note — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in step 28.

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes and the Static Hosts tab refreshes with the configured static hosts displayed.

39 Configure router advertisement, if required.

i Click on the Advertisement tab button.

ii Click on the Create button to add a router advertisement entry. The Router Advertisement (Create) form opens.

iii Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

iv Click on the Prefix tab button.

v Click on the Create button. The Router Advertisement Prefix (Create) form opens.

vi Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Router Advertisement (Create) form reappears.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Router Advertisement (Create) form closes and the L3 Access Interface (Create) form refreshes with the router advertisement entry.

40 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Create button. The ANCP Static Map (Create) form opens with the General tab displayed.

iii Configure the ANCP String parameter.

iv Click on the Select button in the ANCP Policy panel to choose an ANCP policy. The Select ANCP Policy - ANCP Static Map list form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The ANCP Static Map (Create) form closes.

41 Specify queue overrides by clicking on the Override Policy Items tab button.

Note — The Override Policy Items tab contains a number of sub-tabs. However, the sub-tabs that are displayed depend on the port type that you have chosen for this interface.

- If you configured a non-HSMDA port, then the Access Ingress Queues, Access Egress Queues, Ingress Policer, and Egress Policer sub-tabs are active.
- If you configured an HSMDA port, then the Access Ingress Queues, Access Egress HSMDA Queues and Ingress Policer sub-tabs are active.

Set the queue overrides, as described in Procedure 47-44.

42 If the IPv6 Allowed parameter in step 7 is enabled, the DHCPv6 tab is configurable. Configure IPv6 DHCP, if required. Otherwise, go to step 43.

i Click on the DHCPv6 tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

iii Click on the Server tab button.

iv Configure the Server 1 through Server 8 parameters.

v Configure the interface name for each DHCPv6 server that you configured in step iv by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

vi Select an interface from the list and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the L3 Access Interface form refreshes with the interface information.

vii Click on the DHCPv6-Prefix tab button.

viii Click on the Create button. The DhcpRelayV6PrefixDelegation (Create) form opens.

ix Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The L3 Access Interface (Create) form reappears.

43 Click on the OK button. The L3 Access Interface (Create) form closes, and the Site (Create) form reappears with the new interface information displayed in the service navigation tree.

Repeat steps 6 to 43 to create another L3 access interface for the site in the VPRN service.

Note — If you are creating the L3 access interface during service creation, return to Procedure 74-1.

Procedure 74-3 To configure a VPRN network interface

Note — You cannot configure at network interface on a VPRN service if there are any pre-existing interfaces configured on the service. Once a network interface is configured on a VPRN service, no other interface types can be configured on the service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab button.

6 Select a VPRN site from the list and then click on the Properties button. The VPRN Site (Edit) form opens with the General tab displayed.

7 Click on the Routing tab button.

8 On the General subtab, configure the Carrier Carrier VPN parameter.

The Carrier Carrier VPN parameter is only available if there are no other interfaces configured on the site.

9 Click OK on the VPRN Site (Edit) form. You are returned to the VPRN Service (Edit) form.

10 Click on the Network Interfaces tab button and then click on the Create button. The Network Interface (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Class
- Loopback Enabled
- PIM RP Delayed Up Period
- Cflowd Type
- Trusted
- Enable Ingress Flowspec
- LSR IP Load Balancing
- URPF Check State
- URPF Check Mode

12 Click on the Port tab button.

Note — If the Loopback Enabled parameter is selected on the General tab, the Port port tab does not appear. Skip to step 15.

13 Click on the Select button and select a terminating port for the interface from the Select Terminating Port form.

14 Configure the parameters:

- Outer Encapsulation Value
- Auto-Assign ID
- Inner Encapsulation Value

15 Click on the Policies tab button.

i Click on the Select button in the Network Policy panel to list and choose a network policy for the interface. Network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network.

Note — If you select a network policy with a forwarding class mapped to a queue group queue ID, you must ensure that the mapping queue group queue ID is in the selected Queue Group Template Policy.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

ii Click on the Select button beside the Queue Group Template Policy to list and choose a network egress queue group template policy for the interface. Queue group template policies allow SAP or IP interface forwarding classes to be redirected from the typical queue mapping to a shared queue.

Note — You must ensure that the port you selected in step 13 has a network egress queue group with the same name as the Queue Group Template policy created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

iii Click on the Select buttons to list and choose Ingress and Egress ACL filters for the interface. ACL filters are used to filter out IP traffic that matches user-defined criteria.

16 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button next to the Policy ID field and select a policy from the Select NE DoS Protection - Network Interface form.

17 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button.

ii Configure the parameters:

- Administrative State
- Transmit Interval
- Receive Interval
- Echo Interval
- Multiplier

The Transmit Interval, Receive Interval, Receive Interval, Echo Interval, and Multiplier parameters are configurable only when the Administrative State parameter is set to Up.

iii To view local and remote session peers that are managed by the 5620 SAM. Click on the BFD Session tab button. A list of BFD current sessions on the interface appears.

iv Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

v Close the form.

Note — You cannot configure BFD for an interface if BFD is disabled. See chapter 31 for information about enabling and disabling BFD for routing protocols.

18 Click on the ARP tab button.

i Configure the Timeout (seconds) parameter.

ii Click on the Create button to statically associate an IP or MAC address to the interface. The Static ARP (Create) form opens.

Configure the parameters:

- IP Address
- Physical Address

iii Click on the OK button. The Static ARP (Create) form closes.

19 Click on the Addresses tab button to assign IP addresses to the interface:

i Click on the Create button. The IP Address, Routing Instance (Create) form opens.

ii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- IGP Inhibit
- Broadcast Address Format

iii Click on the OK button to save the changes. A dialog appears.

iv Click on the OK button. The IP Address, Routing Instance (Create) form closes. The Network Interface (Create) form reappears with the assigned IP addresses displayed.

20 Click on ICMP tab button and configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

21 Click NTP tab button.

22 Configure the Broadcast parameter.

Note — When the Broadcast parameter is enabled, a time protocol such as NTP or SNTP must be enabled and configured on the device, or the device ignores broadcast time packets received on the interface. See chapter 13 for information about configuring NTP or SNTP on a device.

23 Click on the OK button. The Network Interface [Create] form closes. The VPRN Service (Create) form reappears with the assigned network interface displayed.

Procedure 74-4 To configure a GNE site on a VPRN service

Use this procedure to add a GNE site and GNE service interfaces to an existing VPRN service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the component tree, right-click on VPRN Service and choose Create GNE Site. The Select Network Elements - VPRN Service form opens with a list of available sites.

5 Choose a site and click on the OK button. The GNE Site (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description

7 Click on the Apply button.

8 To configure an interface for the GNE site, perform the following steps:

i Click on the GNE Service Interfaces tab button and then click on the Create button. The GNE Service Interface (Create) form opens with the general tab displayed.

ii Configure the parameters:

- Name
- Description
- Type

iii Click on the Ports tab button and then click on the Select button next to the Interface Index field. The Select Generic NE Interface form appears.

iv Select an interface from the list and click on the OK button. The GNE Service Interface (Create) form reappears with the interface information displayed.

v Configure the parameters:

- Encap Type
- Outer Encapsulation Value
- Inner Encapsulation Value

vi Click on the OK button. The GNE Site (Create) form reappears with the interface information displayed in the service component tree.

9 Click on the Scripts tab button to attach or execute configuration scripts on the GNE site.

The Scripts tab displays the script instances and versions that are applied to the device. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

10 Click on the OK button. The VPRN (Edit) form reappears with the new information displayed in the service component tree.

11 Click on the OK button. The VPRN (Edit) form closes.

You can use the topology maps to view the service. See chapter 5 for more information about service topology maps.

Procedure 74-5 To configure BGP, OSPFv2, OSPFv3, PIM, RIP, or L2TP on a VPRN routing instance

Note — To configure IGMP on a VPRN routing instance, see Procedure 74-6.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
3. Select a VPRN service.
4. Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.
5. On the navigation tree, click on the site to which you want to add the routing instance; expand the entries for that site.
6. Expand the Routing Instance icon.
7. Right-click on the Protocols icon and perform one of the following from the contextual menu:
    a. Choose Create BGP Site to configure BGP on the VPRN routing instance, and then perform steps 4 to 28 of Procedure 31-2.
    b. Choose Create OSPF Site to configure OSPFv2 on the VPRN routing instance, and then perform steps 5 to 19 of Procedure 31-22.
    c. Choose Create OSPF Site to configure OSPFv3 on the VPRN routing instance, and then perform steps 5 to 11 and steps 13 to 19 in Procedure 31-22.
    d. Choose Create PIM Site to configure PIM on the VPRN routing instance, and then perform steps 4 to 81 in Procedure 31-33.
    e. Choose Create RIP Site to configure RIP on the VPRN routing instance, and then perform steps 4 to 15 in Procedure 31-8.
    f. Choose Create L2TP Site to configure L2TP on the VPRN routing instance, and then perform steps 3 to 18 in Procedure 31-30.
8. Click on the OK button. The protocol configuration form closes, and a dialog box appears.
9. Click on the OK button. The VPRN (Edit) form reappears.
10. Click on the OK button. A dialog box appears.
11. Click on the Yes button to confirm the action. The VPRN (Edit) form closes.
12. Close the Manage Services form.

Procedure 74-6 To configure IGMP on a VPRN routing instance

Note — PIM-SSM for IPv6 is currently not supported in VPRN services.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
3. Select a VPRN service.
4. Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.
5. On the navigation tree, click on the site to which you want to add the routing instance; expand the entries for that site.
6. Expand the Routing Instance icon.
7. Right-click on the Protocols icon and choose Create IGMP Site from the contextual menu. The IGMP Site (Edit) form opens with the General tab displayed.
8. Configure the parameters:
   - Administrative State
   - Query Interval (seconds)
   - Last Member Query Interval (seconds)
   - Query Response Interval (seconds)
   - Robust Count
9. Click on the SSM Translation tab button to configure SSM, if required.
   - **i** Click on the Create button to create a new entry. The SSM Translation (Create) form opens.
   - **ii** Configure the parameters:
     - Start Mcast Address
     - End Mcast Address
     - Configured Source
   - **iii** Click on the OK button. A dialog box appears.
   - **iv** Click on the OK button. The new SSM entry appears on the form.
10. Click on the Interfaces tab button to add an interface, if required.
    - **i** Click on the Create button.
    - **ii** Perform steps 4 to 15 of Procedure 31-39.
    - **iii** Click on the OK button. The new interface entry appears on the form.

11 Click on the Group Interfaces tab button to identify an IGMP group interface for a VPRN service, if required.

12 Click on the Create button and configure the parameters in the IGMP Group Interface - Routing Instance (Create) form:

- Description
- Administrative State
- Forwarding Service ID
- Name

13 Click on the OK button. The Group Interfaces tab reappears.

14 Click on the Select button next to the Interface ID field to select a group interface from the Select IGMP Group Interface - IGMP Group Interface - Routing Instance form.

15 Click on the following tab buttons to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

16 Click on the OK button. The protocol configuration form closes, and a dialog box appears.

17 Click on the OK button. The VPRN (Edit) form reappears.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to confirm the action. The VPRN (Edit) form closes.

20 Close the Manage Services form.

Procedure 74-7 To add a Global Route Table to a VPRN site

Packets within a VRF are able to perform a parallel lookup against a Global Route Table (GRT), as well as within the local VRF table. A successful routing table match found in the local VRF is typically preferred over any match found in the GRT. However, a static route can be used to allow for specific prefixes covered by the static route to fail the lookup in the local VRF table, thus resulting in the guaranteed use of a route from the GRT.

The GRT is populated by defining export policies for each participating VPRN service, and the maximum number of routes that are exported from a specific VRF can be limited.

Note — The addition of a GRT to a VPRN service is supported only on a 7450 ESS in mixed mode, and on a Release 8.0 or later 7710 SR or 7750 SR.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the GRT; expand the entries for that site.

5 Right-click on the routing instance to which you want to add the GRT and select Properties. The VPRN Site (Edit) form opens, with the General tab displayed.

6 Click on the Routing tab.

7 Configure the Enable GRT Lookup parameter in the General sub-tab.

8 Click on the GRT Export Policies sub-tab.

9 Configure the Max Number of Exported Policies parameter.

10 Specify up to five export policies by using the Select button to choose policies from the filtered list and then clicking on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The VPRN Site (Edit) form closes and a dialog box appears.

13 Click on the OK button. The VPRN Service (Edit) form closes.

14 Close the Manage Services form.

Procedure 74-8 To add a PIM interface to a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, click on the site to which you want to add the PIM; expand the entries for that site.

6 Expand the Routing Instance icon.

7 Expand the Protocols icon.

8 Right-click on a PIM instance in the service navigation tree and choose Create PIM Interface. The PIM Interface, Routing Instance (Create) form opens.

9 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

10 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

11 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

12 Configure the parameters:

- Description
- Administrative State
- BFD Enabled

13 Click on the Behavior tab button.

14 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Sticky DR Priority

The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

15 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

16 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

17 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

18 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

19 Click on the OK button. A dialog box appears.

20 Click on the OK button.

21 Click on the OK button to close the VPRN (Edit) form. A dialog box appears.

22 Click on the Yes button to confirm the action. The VPRN (Edit) form closes.

23 Click on the Close button to close the Manage Services form.

Procedure 74-9 To add an IGMP interface to a VPRN

Note — IGMP must be enabled at the routing instance level before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the IGMP interface; expand the entries for that site.

5 Right-click on an IGMP instance and choose Create IGMP Interface. The IGMP interface, Routing Instance (Create) form opens with the General tab displayed.

6 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

7 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

8 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

9 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

10 Click on the Behavior tab button to add an import policy, if required.

11 Click on the Select button in the Properties panel to choose an import policy. The Select - IGMP Interface form opens.

12 Configure the filter criteria. A list of import policies appears at the bottom of the Select - IGMP Interface form.

13 Choose an import policy from the list and click on the OK button. The Select - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form reappears.

14 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

15 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

16 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

17 Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

18 Click on the Static Group/Source tab button to add a static multicast group or source, if required.

19 Click on the Create button to add a new entry. The StaticGrpSrc, Routing Instance (Create) form opens.

20 Configure the parameters:

- Static Multicast Group
- Static Source

21 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

22 Click on the OK button to confirm the action.

23 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form. A dialogue box opens.

24 Click on the OK button to confirm the action. The VPRN (Edit) form reappears.

25 Click on the OK button to close the VPRN (Edit) form. A dialog box appears.

26 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

27 Close the Manage Services form.

Procedure 74-10 To create a VPRN spoke SDP binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens.

4 On the navigation tree, click on the site to which you want to add the spoke SDP binding; expand the entries for that site.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding from the contextual menu. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the SDP binding:

   i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

   ii Configure the filter criteria. A list of interfaces appears at the bottom of the form.

   iii Select an entry and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the source interface information.

   iv Configure the parameters:

   - VC ID
   - Auto-Assign ID
   - VC Type
   - Enable Hash Label
   - Enable Signal Capability

   The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated.

7 Specify a destination node for the spoke SDP binding:

   a If the destination node is a managed node, choose from a list of managed nodes.

      i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

      ii Select a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

   b If the destination node is an unmanaged node, specify its system ID in the Tunnel Termination Site parameter.

8 Configure the Description parameter.

9 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Specify an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

11 Choose one of the following AA transit policy types, if required.

Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Select a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

12 To configure custom object attributes for AA reporting to the 5670 RAM, perform the following steps:

i Click on the 5670 RAM Parameters tab button.

ii Click on the Reporting tab button.

iii Click on the Create button. The AA Reporting (Create) form opens.

iv Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

v Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

vi Click on the General tab button.

13 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

> **Note —** You can create a return tunnel only between sites that are within the same service. If the sites are not in the same service, the Return tab does not appear.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

14 Click on the States tab button.

15 Configure the Administrative State parameter.

16 Associate a MEP to the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Create button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

17 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 21.

18 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

19 Click on the AIS tab button.

20 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

21 Click on the OK button. A dialog box appears.

22 Click on the OK button. The MEP (Create) form closes.

23 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

24 Click on the OK button.

Procedure 74-11 To create an L2 SDP spoke termination on a VPRN service

Ensure that a service and site have been created in the VPRN. To terminate an L2 service on a VPRN SDP spoke, you must identify the VC and an interface belonging to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens.

4 On the navigation tree, click on the site to which you want to create an L2 SDP spoke termination; expand the entries for that site.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Click on the Select button in the Source Interface panel to select an interface with no port assigned.

If you are creating this spoke SDP binding for use with an IP mirror interface, select the required IP mirror interface as the source interface.

7 Click on the OK button. The Select Interface - Spoke SDP Bindings form closes and the Spoke SDP Bindings (Create) form reappears with the interface information displayed.

8 Specify a destination node for the spoke SDP binding by performing one of the following tasks.

a If the destination node is a managed node, choose from the list of managed nodes.

i Click on the Select button in the Tunnel Termination Site panel. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

c If you are configuring IP mirroring, select a mirror source site as the tunnel termination site.

9 Configure the parameters:

- Auto-Assign ID
- VC ID
- VC Type
- Ingress Label
- Egress Label
- Enable Hash Label
- Enable Signal Capability

  The Enable Hash Label and Enable Signal Capability parameters can only be configured for spoke-SDP bindings that are access interface terminated. They cannot be configured on mirroring interfaces.

If you are configuring IP mirroring, set the VC ID parameter to the mirror service ID.

10 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto-Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

11 Select an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

12 Choose one of the following AA transit policy types, if required.

Note 1 — You can only associate one AA transit policy type with a service object.

Note 2 — You can bind a transit policy to only one L3 access interface or spoke SDP binding per node.

Note 3 — The transit policy and the application profile must belong to the same application assurance group or partition.

a Associate an AA transit IP policy with the service object:

i Click on the Select button in the Transit IP Policy panel. The Select Transit IP Policy form opens.

ii Select a transit IP policy and click on the OK button.

b Associate an AA transit prefix policy with the service object:

i Click on the Select button in the Transit Prefix Policy panel. The Select Transit Prefix Policy form opens.

ii Select a transit IP policy and click on the OK button.

13 Click on the States tab button.

14 Configure the Administrative State parameter.

15 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter. If you are configuring IP mirroring, you can optionally select an ingress IP filter. This is a packet mirroring option which specifies that packets matching the IP filter are mirrored to the mirror destination. Click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

16 If you are configuring IP mirroring, go to step 18.

17 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

18 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

19 Click on the OK button. The VPRN (Edit) form reappears with the new information displayed in the service navigation tree.

Procedure 74-12 To add a subscriber interface to a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Sreach button. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN Service Subscriber (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the subscriber interface; expand the entries for that site.

5 Right-click on the Subscriber Interfaces icon and choose Create VPRN Subscriber Interface. The VPRN Subscriber Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address
- Tunnel Fault Notification

The Tunnel Fault Notification parameter is configurable on interfaces where the device has ports configured in access or hybrid mode with Q in Q encapsulation.

If you are configuring a facility tunnel MEP, Tunnel Fault Notification must be set to Accept, in order to receive the fault notification from the facility tunnel MEP.

Note 1 — The Name value for a subscriber interface must be unique in the context on the VPRN Service Site. That is, there cannot be another L3 access interface, subscriber interface, or group interface with the same name on the same VPRN site.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

7 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed and IPv6 Delegated Prefix Length parameters.

- IPv6 Allowed
- IPv6 Delegated Prefix Length
- Admin Link Local Address

The Admin Link Local Address parameter is only configurable when the IPv6 Allowed parameter is enabled.

ii Click on the IPv6 Subscriber Prefixes tab button.

iii Select a subscriber prefix from the list and click on the Properties button, or click on the Create button to create a new subscriber prefix.

iv In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

8 Configure the Interface Class parameters, if required.

i Configure the Class parameter.

ii If you selected a value of Unnumbered for the Class parameter, configure the Unnumbered Type parameter.

iii Configure the Interface Name parameter or the IP Address parameter.

9 Perform one of the following:

a Create a subscriber interface for a wholesale and retail VPRN.

When you configure the routing instance for the VPRN, you can set the Type parameter to Subscriber Split Horizon to enable the forwarding service and forwarding subscriber information. The subscriber split horizon VPRN controls the flow of traffic for wholesale subscriber applications. See Procedure 74-1 for more information on how to configure this parameter.

Note — You cannot create a group interface under a forwarding subscriber interface.

Go to step 10.

b Create a subscriber interface for a traditional VPRN. Go to step 12.

10 Assign a forwarding service to the subscriber interface if you are configuring a wholesale and retail configuration for the VPRN.

i Click on the Select button in the Forwarding Service panel to choose a service. The Select Forwarding Service - VPRN Subscriber Interface form opens.

ii Select a service and click on the OK button. The Select Forwarding Service - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the service information displayed.

iii Configure the Private Retail Subnet parameter that appears after you have assigned a forwarding service.

11 Assign a forwarding subscriber interface to the VPRN subscriber interface.

i Click on the Select button in the Forwarding Subscriber Interface panel to choose a subscriber. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form opens.

ii Select a subscriber and click on the OK button. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the subscriber information displayed.

12 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Addresses tab button.

ii Click on the Create button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Track SRRP Instance
- Hold Up Time (milliseconds)
- Gateway IP Address
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you want to create.

13 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button.

ii If you specified a forwarding service in step 10, the General tab is configurable. Configure the parameters that define the forwarding service information. Otherwise go to step vii.

- Enable DHCP Relay
- Description
- Lease Populate

iii If you specified a forwarding service in step 10 and depending on the type and version of the device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step vii.

iv Click on the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Select a policy and click on the OK button. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form closes, and the VPRN Subscriber Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- IP Address
- Use as source

viii Click on the Server tab button.

ix Configure the parameters.

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

x Click on the Client Applications tab button.

xi Configure the Client Applications parameter. You can enable either or both of the PPPoE or DHCP choices.

14 Configure PPPoE for the interface, if required.

Note — PPPoE is only configurable on a VPRN subscriber interface if the interface is a retailer interface.

i Click on the PPPoE tab button.

ii Configure the parameters:

- Description
- Session Limit

15 Configure the ARP host for the interface, if required.

Note — The ARP host is only configurable on a VPRN subscriber interface when the interface is a retailer interface.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit

16 Click on the OK button. The VPRN Subscriber Interface (Create) form closes, and a dialog box appears.

17 Click on the OK button. The VPRN (Edit) form reappears with the new subscriber interface displayed in the service navigation tree.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The VPRN (Edit) form closes, and the Manage Services form reappears.

20 Close the Manage Services form.

Procedure 74-13 To add a group interface to a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the group interface; expand the entries for that site.

5 Right-click on the subscriber interface to which you want to add a group interface, and choose Create VPRN Subscriber Interface. The VPRN Subscriber Interface (Create) form opens with the General tab displayed.

6 Click on the Group Interfaces tab button.

7 Click on the Create button and the VPRN Group Interface (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- LNS
- IPv6 Allowed
- QoS Route Lookup IPv4
- QoS Route Lookup IPv6

Note — The LNS parameter defines the type of group interface (regular or LNS). This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes and an LNS group interface does not allow PPPoE configuration or SAPs.

9 Configure IPv6 router advertisement and DHCPv6 on the group interface, if required.

i Configure the IPv6 Allowed parameter.

ii Click on the IPv6 Advertisement tab button and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Life Time
- Lifetime (seconds)

iii Click on the DHCPv6 tab button.

iv Click on the Select button and select a local user database from the Select Local User Database form.

v Click on the Proxy Server tab button and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Life Time
- Preferred Life Time
- Client Applications

vi Click on the Relay tab button and configure the parameters:

- Administrative State
- Description
- Remote ID
- Client Applications

vii Configure the DHCP Server 1 through DHCP Server 8 parameters:

- Server 1 through Server 8
- Configure the interface name for each DHCPv6 server by clicking on the Select button in the Zone Index panel. The Select Zone Index - GrplfDhcpv6RelayCfg form opens with a list of local L3 access interfaces.
- Select an interface from the list and click on the OK button. The Select Zone Index - GrplfDhcpv6RelayCfg form closes and the VPRN Group Interface form refreshes with the interface name.

Note — If you have entered a Unicast address, then the Interface Name parameter is not required.

10 Click on the Anti-Spoofing tab button.

11 Configure the ARP Populate parameter.

12 Click on the Subscriber Management tab button.

13 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

14 Configure ICMP for the group interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

15 Configure ARP for the group interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 1

16 Configure IPv4 DHCP relay for the group interface, if required.

i Click on the DHCP tab button. The DHCP form opens with the General tab displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof MAC Address
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step x.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Select a policy and click on the OK button. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the policy name information displayed.

vii Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

viii Configure the filter criteria. A list of available databases appears.

ix Select a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the database name information displayed.

x Click on the Server tab button.

xi Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

xii Click on the Client Applications tab button.

xiii Configure the Client Applications parameter.

17 Click on the PPP tab button.

18 Configure the Description and Administrative State parameters:

19 Click on the Select button in the PPPoE Policy panel. The Select PPPoE Policy form opens.

20 Select a PPPoE policy from the list and click on the OK button. The Select PPPoE Policy form closes.

21 Click on the Select button in the PPPoE Local User DB panel. The Select PPPoE Local User DB form opens.

22 Select a PPPoE Local User DB from the list and click on the OK button. The Select PPPoE Local User DB form closes.

23 Click on the Select button in the PPP Policy panel. The Select PPP Policy form opens.

24 Select a PPP policy from the list and click on the OK button. The Select PPP Policy form closes.

25 Click on the Select button in the PPP Local User DB panel. The Select PPP Local User DB form opens.

26 Select a PPP Local User DB from the list and click on the OK button. The Select PPP Local User DB form closes.

27 Configure the remaining parameters:

- Session Limit
- Session Limit per SAP

28 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval (minutes)
- SAP ARP Host Limit

29 If you set the LNS parameter to TRUE in step 8, perform the following steps to configure LNS for the group interface.

> **Note —** After you create an LNS group interface, you must configure the L2TP tunnel group profile or tunnel profile to terminate sessions for the LNS group interface that you just created; see Procedure 31-30. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab button.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens with a list of available profiles.

iv Choose a subscriber profile from the list and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens with a list of available SLA profiles.

vi Choose an SLA profile from the list and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens with a list of available subscriber identification policies.

viii Choose a subscriber identification policy from the list and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens with a list of available default application profiles.

x Choose a default application profile from the list and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the default application profile displayed.

30 Configure the Default Subscriber Identification String parameter.

31 Click on the Service Access Points tab button to configure SAPs for the group interface.

32 Click on the Create button. The VPRN Service Access Point (Create) form opens with the General tab displayed.

33 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

34 Click on the Port tab button.

35 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

36 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

37 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses dot1q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

38 Assign ingress and egress QoS policies to the SAP, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service navigation tree, choose Properties, and configure the parameters on the appropriate tab.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use SAP ID as Subscriber ID

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is BCP dot1q, dot1q, or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPRN Service Access Point form opens.

iv Configure the filter criteria and click on the Search button. A list of available ingress policies appear.

v Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 36 has the access ingress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

vi Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPRN Service Access Point form opens.

vii Configure the filter criteria and click on the Search button. A list of available egress policies is displayed.

viii Select an egress QoS policy and click on the OK button. The Select Egress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the egress QoS policy information displayed.

Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 36 has the access egress queue group with the same name created on it.

See Procedure 20-1 in chapter 20 for more information about how to configure Ethernet ports. See chapter 46 for more information about queue group template policies.

39 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 41.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP earlier in the procedure.

40 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.

Note — The Aggregation parameter is not configurable if the port you selected in step 36 is an HSMDA port.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — The Frame-Based Accounting parameter is not configurable if the port you selected in step 36 is an HSMDA port.

Note 3 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPRN Service Access Point form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

vi Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

vii If the port you selected in step 36 is an HSMDA port, go to step 41.

viii Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPRN Service Access Point form opens.

ix Select an egress scheduler and click on the OK button. The Select Egress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the egress scheduler information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xi Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the egress policer control policy information displayed.

xii Go to step 41.

b Specify that an aggregation scheduler policy is applied to the SAP.

i Set the Aggregation parameter to on.

Note — You cannot specify an access scheduler policy if the port you selected in step 36 is an HSMDA port. Go to step 41.

ii Configure the Frame-Based Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPRN Service Access Point form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

41 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - VPRN Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - VPRN Service Access Point form.

42 Click on the Accounting tab button to assign an accounting policy to the SAP.

i Configure the Collect Accounting Statistics parameter.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPRN Service Access Point form opens.

iii Select an accounting policy and click on the OK button. The Select Accounting Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the accounting policy information displayed.

43 Click on the Anti-Spoofing tab button to configure anti-spoofing for the SAP.

i Configure the Anti-Spoofing parameter.

To configure residential subscriber management for static hosts, the Anti-Spoofing parameter must be set to at least IP-address matching, or optionally, to IP- and MAC-address matching.

ii Click on the Static Hosts tab button to add a static host to the SAP.

iii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iv Click on the Create button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification

vi Configure residential subscriber management for the static host.

vii Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step 44.

viii Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

ix Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

x Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

xi Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

xii Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

44 Click on the OK button. A dialog box appears.

45 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

46 Assign a DoS protection policy to the SAP, if required.

Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - VPRN Service Access Point form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - VPRN Service Access Point form closes and the policy ID is displayed on the L3 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

47 Click on the Subscriber Management tab button to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group
- Disable Router Alert Check

v You can click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab button.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Select a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Select an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Select a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Select an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Select a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Select an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Select an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

xxii Click on the Subscriber Hosts tab button to view active hosts for the subscriber instance, if required.

48 Configure ATM on the SAP, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the VPRN Service Access Point (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the VPRN Service Access Point (Create) form refreshes with the egress ATM policy information displayed.

49 Click on the OK button. The VPRN Service Access Point (Create) form closes and a dialog box appears.

50 Click on the OK button. The VPRN Group Interface (Create) form refreshes to display the SAP.

51 To configure an additional SAP in the group interface, go to step 32.

52 Click on the SRRP tab button.

53 Configure the parameters in the Routing panel:

- Enabled
- Hold Time (seconds)

54 Click on the Create button in the SRRP Instance panel. The SRRP Instance (Create) form opens with the General tab displayed.

55 Configure the parameters:

- SRRP ID
- Description
- Administrative State

56 Click on the Select button in the Operational Group panel. The Select Monitored Group Name - SRRP Instance form opens.

57 Select a Monitored Group Name and click on the OK button. The Select Monitored Group Name - SRRP Instance form closes.

58 Configure the Priority Step parameter.

59 Click on the Behavior tab button.

60 Configure the General parameters:

- Gateway MAC Address
- Keep Alive Interval
- Priority
- Preempt
- FIB Population Mode
- One Gratuitous ARP Per SAP

61 Click on the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

62 Select the SAP you want to use for the in-band messaging between the sites and click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

63 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens.

64 Select an entry and click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

65 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 2 - SRRP Instance form opens.

66 Select an entry and click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

67 Click on the OK button. The SRRP Instance (Create) form closes and a dialog box appears.

68 Click on the OK button.

69 Click on the OK button. The VPRN Group Interface (Create) form closes and a dialog box appears.

70 Click on the OK button. The VPRN (Edit) form refreshes to display the SAP below the group interface.

71 Click on the OK button. A dialog box appears.

72 Click on the Yes button. The VPRN (Edit) form closes.

73 Close the Manage Services form.

Procedure 74-14 To collect and view PPP ATM SAP statistics and information for a VPRN group interface

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting statistics.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose VPRN Service (VPRN) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of VPRN services appears.

4 Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 On the navigation tree, click on a group interface. The VPRN Group Interface (Edit) form opens.

6 Click on the Statistics tab button.

7 Choose PPP ATM SAP (Service Management) from the object drop-down list.

8 Click on the Collect button to collect the PPP ATM SAP statistics.

9 Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

10 View the statistics information.

11 Click on the Close button to close the statistics record form.

12 Repeat steps 9 to 11 for each statistics record that you want to view.

13 Close the VPRN Group Interface (Edit) form.

14 Close the VPRN Service (Edit) form.

15 Close the Manage Services form.

Procedure 74-15 To add an IP mirror interface to a VPRN

Perform this procedure to configure an IP mirror interface in a VPRN service. This is a spoke terminated interface used to receive mirrored packets from a remote source.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 On the navigation tree, click on the site to which you want to add the IP mirror interface; expand the entries for that site.

5 Right-click on IP Mirror Interfaces and choose Create IP Mirror Interface. The IP Mirror Interface (Create) form opens.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

Note — The Name value for an IP mirror interface must be unique in VPRN site. There cannot be another L3 access interface, subscriber interface, or group interface with the same name on the VPRN site.

7 Click on the OK button. The IP Mirror Interface (Create) form closes and a dialog box appears.

8 Click on the OK button. The VPRN (Edit) form reappears with the IP mirror interface displayed in the service navigation tree.

9 Create a spoke SDP binding for the interface by performing steps 5 to 19 of Procedure 74-11.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPRN (Edit) form closes, and the Manage Services form reappears.

12 Close the Manage Services form.

Procedure 74-16 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

4 Create the redundant interface used for SRRP out-of-band messaging between the two NEs.

Note 1 — The two sites that participate in the dual homing configuration do not have to be part of the same service.

Note 2 — Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that are participating in the redundant configuration.

Note 3 — Ensure that all subscriber interface IP addresses have a gateway address configured on them.

i On the navigation tree, click on the sites to which you want to add the redundant pair; expand the entries for that site.

ii Right-click on Redundant Interfaces for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iv Click on the Addresses tab button.

v Click on the Create button. The IP Address (Create) form opens.

vi Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Remote IP Address
  This must be on the same subnet as the redundant interface IP address of the current site. For example, if the IP address of the current site is 7.7.7.7, with a prefix length of 24, then the redundant interface IP address of the remote site must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.
- Broadcast Address Format

vii Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

viii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses listed.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Redundant Interface (Create) form for the current site closes.

5 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 4 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site. See Procedure 74-10 for more information.

6 Assign the Redundant Interface to the Group Interface for the current site.

i On the navigation tree under the Subscriber Interface, right-click on the Group Interface you want to use and choose Properties. The VPRN Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface block. The Select Redundant Interface - VPRN Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of Redundant Interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 4. The Select Redundant Interface - VPRN Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The VPRN Group Interface (Edit) form closes.

7 Create an SRRP Instance for the current site.

i On the navigation tree under Group Interfaces, right-click on the SRRP Instances item for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
- Description
- Administrative State

Note — The SRRP ID value must be the same for the current and remote sites.

iii Click on the Behavior tab button.

iv Configure the General parameters:

- Gateway MAC Address Default is 00-00-00-00-00-00.
- Keep Alive Interval
- Priority
- FIB Population Mode

v Configure the Message Path by clicking the Select button adjacent to the Port field. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site. Select the SAP you want to use for the in-band messaging between the sites.

vi Configure the Policy Pointers for the SRRP Instance, if required.

vii Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.

viii Click on the OK button. The VPRN (Edit) form reappears with the SRRP Instance displayed.

8 Click on the Turn Up button to activate the SRRP instance.

9 Repeat steps 4 to 8 for the remote site.

Note 1 — When you repeat steps 4 to 8 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's navigation tree. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote node.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The VPRN (Edit) form closes.

Procedure 74-17 To create an OSPF sham link

Perform this procedure to create an intra-area OSPF sham link between two VPRN sites. See "OSPF sham link support" in section 74.1 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 On the navigation tree, choose the first site that to participate in the sham link. If you need to create the site, perform steps 7 to 82 of Procedure 74-1.

6 Choose an L3 access interface for the site. If you need to create the L3 access interface, perform steps 5 to 43 of Procedure 74-2.

7 Configure OSPFv2 for the site. Perform to steps 6 to 9 of Procedure 74-5. Ensure that you select sub-step b in step 7.

8 Right-click on the OSPFv2 icon under the Protocols icon and choose Create Sham Link. The ShamLink (Create) form opens with the General tab displayed.

9 Click on the Select button to configure the Remote Neighbor IP Address parameter. This is the IP Address of the other site participating in the sham link.

10 Click on the Select button in the Interface block to configure the Interface Name parameter. The Select Interface - ShamLink form opens.

11 Click on the Search button.

12 Select an interface from the displayed list and click on the OK button. The Select Interface - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Interface Name displayed.

13 Click on the Select button in the Area block to configure the Area ID parameter. The Select Area - ShamLink form opens.

14 Click on the Search button.

15 Select an area from the displayed list and click on the OK button. The Select Area - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Area ID displayed.

16 Configure the Administrative State parameter.

17 Click on the Protocol Properties tab button.

18 Configure the parameters:

- Metric
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

19 The Authentication tab is configurable, depending on the OSPF version. Click on the Authentication tab button to configure authentication for the sham link, if required. Otherwise, go to step 22.

20 Configure the Authentication Type parameter. Perform one of the following:

a Click on the Authentication Type menu button and choose MD5-based Authentication from the drop-down menu.

i Click on the Create button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Click on the Authentication Type menu button and choose Simple Password from the drop-down menu.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

21 You can click on the Virtual Neighbor tab button to view OSPF configuration information on neighbor sites, if required.

22 Click on the OK button. A dialog box appears.

23 Click on the Yes button. The ShamLink (Create) form closes, and the 5620 SAM displays an icon for the new sham link in the navigation tree.

24 Repeat steps 5 to 23 for the second site participating in the sham link.

25 Click on the OK button. A dialog box appears.

26 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

27 Click on the Close button to close the Manage Services form.

Procedure 74-18 To run an OAM validation test for a VPRN service

An OAM validator test suite must be created for the tested entity. See chapter 78 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the More Actions button and choose Validate. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

- **i** Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.
- **ii** Configure the filter criteria. A list of OAM validator test suites appears.
- **iii** Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPRN (Edit) form.

15 Close the Manage Services form.

Procedure 74-19 To view the service topology map associated with a VPRN service

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
3. Select a VPRN service and click on the Topology View button. A Topology View dialog box appears.
4. Click on the Yes button to proceed. The Service Topology - map opens.

   See chapter 5 for more information about service topology views.

Procedure 74-20 To view the VPRN service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.
3. Select a service and click on the Properties button. The VPRN (Edit) form opens.
4. View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.
5. Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.
6. Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.
7. Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.
8. Close the VPRN (Edit) form.
9. Click on the Close button to close the Manage Services form.

Procedure 74-21 To view DHCPv6 leases

This procedure describes how to view the DHCPv6 prefixes that the server has given out.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site where you want to view DHCPv6 leases; expand the entries for that site.

5 Choose Routing Instance from the navigation tree.

6 Click on the Local DHCP Servers tab button.

7 Click on the DHCP V6 tab button. The list of associated DHCPv6 servers is displayed.

8 Select a DHCPv6 server from the list and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

9 Click on the More Actions button and choose Show Leases. The DHCPv6 Server Show Leases form opens.

10 Perform one of the following:

   a To view the entire list of leases that are active on the DHCPv6 server, click OK.

   b To view the lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server and click OK.

   Note — If the prefix does not exist in the list of leases, a message displays.

   c To view the detailed lease information for a specific prefix, enter the IP address in the Prefix parameter for the particular DHCPv6 server, select the Detail check box, and click OK. The form displays the CLI details for the specific prefix.

11 Close the DHCPv6 Server Show Leases form.

12 Close the Local DHCPv6 Server (Edit) form.

Procedure 74-22 To view DHCPv6 log events

This procedure describes how to view lease not owner and pool unknown log events for local DHCPv6 servers.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

4 On the navigation tree, click on the site where you want to view DHCPv6 log events; expand the entries for that site.

5 Choose Routing Instance from the navigation tree.

6 Click on the Local DHCP Servers tab button.

7 Click on the DHCP V6 tab button. The list of associated DHCPv6 servers is displayed.

8 Select a DHCPv6 server from the list and click on the Properties button. The Local DHCPv6 Server (Edit) form opens with the General tab displayed.

9 Click on the Logs tab button. The Lease Not Owner Log and Pool Unknown Log tabs display.

10 Click on the tab button for the type of log that you wish to display. Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

11 Configure the filter criteria and click on the Search button. A list of event logs appears.

12 Select a log entry and click on the Properties button. The Log form opens.

13 View the log entry.

14 Close the Log form.

15 Close the Local DHCPv6 Server (Edit) form.

Procedure 74-23 To modify a VPRN service

Caution 1 — Modifying parameters can be service-affecting.

Caution 2 — The behavior of the VPRN service may become unpredictable if modifications to the configuration affect the IPsec portion of the service configuration. For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies are deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using CLI scripts or the CLI before the VPRN service can be deleted from the 5620 SAM.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Tests tab — allows the creation and execution of service-specific diagnostic tests
- Sites tab — lists the sites that are included in the service
- L3 Access Interfaces tab — lists the L3 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Addresses tab — lists the IP addresses that are associated with the service

Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

To configure items in the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 74-24 To modify a VPRN service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the navigation tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be viewed, created, or modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 36.
- Viewing the route target topology. Go to step 44.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create VPRN Site option.

The Select Network Elements form appears.

5 Select one or more sites to add to the service and click OK. The VPRN Site (Create) form for the new site is displayed. If you selected more than one site, the VPRN Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The VPRN Site (Create) (or VPRN Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedure 74-1 for detailed site configuration information.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating site components

9 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPRN L3 Access Interface. Go to step 10.
- Tunnel Interface. Go to step 15.
- VPRN Subscriber Interface. Go to step 20.
- Redundant Interface. Go to step 24.
- IP Mirror Interface. Go to step 28.
- Video Interface. Go to step 32.

10 If you choose to create a VPRN L3 Access Interface, then the VPRN L3 Access Interface (Create) form is displayed.

11 Configure the Name parameter on the General tab.

12 Click on the Port tab and assign a port to the interface.

Refer to Procedure 74-2 for detailed information on further configuring the interface, if required.

13 Click OK. The VPRN L3 Access Interface (Create) form closes and the new L3 access interface is displayed in the topology view.

14 Go to step 35.

15 If you choose to create a tunnel interface, then the Tunnel Interface (Create) form is displayed.

16 Configure the Name parameter on the General tab.

17 Click on the Port tab and assign a port to the interface.

Refer to Procedure 35-6 in Chapter 35 for detailed information on further configuring the interface, if required.

18 Click OK. The Tunnel Interface (Create) form closes and the new tunnel interface is displayed in the topology view.

19 Go to step 35.

20 If you choose to create a VPRN Subscriber Interface, then the VPRN Subscriber Interface (Create) form is displayed.

21 Configure the Name parameter for the interface.

Refer to Procedure 74-12 for detailed information on further configuring the interface, if required.

22 Click OK. The VPRN Subscriber Interface (Create) form closes and the new subscriber interface is displayed in the topology view.

23 Go to step 35.

24 If you choose to create a Redundant Interface, then the Redundant Interface (Create) form is displayed.

25 Configure the Name parameter for the interface.

Refer to Procedure 74-16 for detailed information on further configuring the interface, if required.

26 Click OK. The Redundant Interface (Create) form closes and the new redundant interface is displayed in the topology view.

27 Go to step 35.

28 If you choose to create an IP Mirror Interface, then the IP Mirror Interface (Create) form is displayed.

29 Configure the Name parameter for the interface.

Refer to Procedure 74-15 for detailed information on further configuring the interface, if required.

30 Click OK. The IP Mirror Interface (Create) form closes.

31 Go to step 35.

32 If you choose to create a Video Interface, then the Video Interface (Create) form is displayed.

33 Configure the Name parameter for the interface.

Refer to Procedure 36-1 in Chapter 36 for detailed information on further configuring the interface, if required.

34 Click OK. The Video Interface (Create) form closes and the new video interface is displayed in the topology view.

35 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating spoke SDP bindings

36 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

37 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

38 Enable the Auto-Select Transport Tunnel parameter.

39 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 74-10 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

40 Assuming that the spoke SDP binding was successfully created in step 39, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

41 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

42 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 33 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

43 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Viewing the route target topology

44 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Highlight Route Target Topology option.

This option essentially draws dotted lines to represent the route target topology between NEs. For example, for two NEs A and B, if the import and export route targets match, then two dotted lines will be drawn on the map. One will represent the route target going from A to B, and the other from B to A.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

46 Close the Service Topology form.

47 Close the Manage Services form.

Procedure 74-25 To delete a VPRN service

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

Note 1 — You cannot delete a VPRN service when IPsec security policies, interfaces, or tunnels are configured. See the appropriate node documentation for more information about modifying or deleting IPsec configurations.

For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies is deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using the CLI scripts or through the CLI before the VPRN service can be deleted from the 5620 SAM.

Note 2 — The L3 interface properties for the IPSEC SAP cannot be configured using the 5620 SAM.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

- **a** For services with a low priority, go to Step 5.
- **b** For services with a medium priority, configure the “Enter the highest priority of the service being deleted” text field by typing: Medium. Go to Step 5.
- **c** For services with a high priority, configure the “Enter the highest priority of the service being deleted” text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

75 — PW routing and dynamic MS-PW service management

75.1 PW routing and dynamic MS-PW service management overview

Service providers require a solution for interconnecting customer sites that span different domains, such as MAN-WAN or Inter-AS (in the same Service Provider or Inter-Provider). The 5620 SAM supports two methods for interconnecting customers sites:

- PW routing
- MS-PW routing

PW routing

Prior to 5620 SAM release 9.0 R5, the Alcatel-Lucent SR 7x50 provided inter-domain services for VLL through the use of VLL spoke switching, which allows creation of a VLL service by cross-connecting two spoke SDPs. However, this required statically configuring the PW switching points at the gateway S-PEs between domains. See “VLL spoke switching” in chapter 70 for more information.

MS-PW routing

Multi-Segment Pseudo-Wire routing provides solutions for inter-domain services by using dynamic MS-PW routing and signaling, in which the switching points are automatically instantiated in the Switching-Provider Edge (S-PE) NEs. The path of the MS-PW is dynamically signaled end-to-end by T-LDP, using PW routing information stored in the S-PEs by MP-BGP. Per-PW configuration is only required at the endpoints of the MS-PW in the Termination-Provider Edge (T-PE) NEs.

Dynamic MS-PWs are characterized by the following:

- They are supported for VLL Epipe services
- Dynamic and static routes, as well as explicit paths for MS-PWs are supported
- Dynamic MS-PWs may be established across LDP or RFC 3107 labeled BGP SDPs
- Dynamic MS-PWs may be used as a part of a set of PWs for PW redundancy, including MC-LAG. Diverse routes for the active and standby MS-PWs can be configured by using explicit paths, or dynamically by using a BGP route distinguisher.
- Diverse routes for the active and standby MS-PWs can be achieved by using explicit paths or dynamically using a BGP route distinguisher.

Dynamic MS-PWs are supported on all NE release 9.0 R3 7750 SR, 7450 ESS, and 7710 SR chassis that support Epipe services.

Dynamic MP-PW services

Spoke SDP FEC configuration will bind a service to an existing Service Distribution Point (SDP), using a dynamic MS-PW. When using dynamic MS-PWs, the particular SDP to bind to is automatically selected based on the Target Attachment Individual Identifier (TAII) and the path to use, specified under the Spoke SDP FEC. The selected SDP will terminate on the first hop S-PE of the MS-PW. Therefore, an SDP should be defined that can reach the first hop of the MS-PW. The SR 7x50 will create a spoke SDP binding in order to associate an SDP with a service. If an SDP to that does not exist, the SR 7x50 will create one based on the parameters specified in the spoke SDP FEC (such as the SAII/TAII, Path, PW template, and so forth). The Creation Mode attribute for such an SDP will indicate Multi-Segment PW.

This differs from the regular spoke SDP binding creation in that it creates a spoke SDP binding using a PW with the FEC128. However, the Spoke SDP FEC enables PWs with other FEC types to be used. At release 5620 SAM 9.0 R5, only FEC129 is supported.

Spoke SDP FEC configuration is currently only applicable to an Epipe site. It can be configured under the Epipe service or at a service endpoint of an Epipe site, with or without ICB. The creation under an Epipe service is demonstrated in the following steps.

75.2 Workflow to configure PW routing and dynamic MS-PW services

The following workflow lists the high-level steps required to configure PW routing and dynamic MS-PW services. Enabling MS-PW support requires configuration in the following areas:

- network commissioning
- SR NE pre-provisioning
- dynamic MS-PW service
- optional PW routing and MS-Service tasks

Network commissioning

1 To use PW routing to establish dynamic pseudo-wires from source to destination, without using static routes and a specified path:

a Enable BGP on the routing instance of the required node. See Procedure 31-1 for more information.

b Configure the BGP Family parameter to include the options MS-PW and IPv4. This must be done on the BGP site, associated BGP groups, and BGP peers.

Refer to the following procedures:

- BGP Site configuration: See step 17 in Procedure 31-2
- BGP Peer Group configuration: See step 13 in Procedure 31-4
- BGP Peers configuration: See step 12 in Procedure 31-5

2 If more than one equal cost route is required for the PW routing, configure the following:

a In the routing instance for the required NE, set the Maximum Number of Equal Cost Routes parameter to a value greater than 1. See step 18 in Procedure 30-2.

b For the required BGP Site, set the Multi Path parameter to a value greater than 1. See step 6 in Procedure 31-2.

3 Configure a routing policy with the Family parameter having the MS-PW option enabled. This will then be exported under the BGP site. See step 21 in Procedure 30-11.

4 If path diversity is required for primary/standby MS-PWs, perform the following:

a Configure a routing policy having multiple statement entries, each associated with a different community, from a different neighbour, with family including MS-PW and a local preference. The communities configured here are used further on in the procedure when configuring a MS-PW local prefix. See Procedure 30-11 for more information, with attention to steps 22 and 23.

b Import the above policy under the BGP site. See Procedure 31-2 for more information.

5 If there are ASBRs, set Next Hop Self to True under each peer group. For example, set one for the inner-AS and one for the external-AS. Without this setting, the SDPs created by MS-PW routing only reach to the BGP interface's IP address, but not the system ID. See step 9 in Procedure 31-4. Refer also to Chapter 74 for information on ASBRs.

6 If all T-PEs and S-PEs are within the same AS, then the S-PEs must be configured as route reflectors (RR). Perform the following:

a Set the Cluster ID parameter on the BGP site or BGP peer group that includes the T-PEs as BGP peers on the S-PE. See step 4 in Procedure 31-2.

Note — Two T-PEs can not be configured as BGP peers to each other. They must be configured as BGP peers of the RR.

b Configure a routing policy with Advertise Next Hop Self set to true and Action set to Accept, and then export this policy under the BGP site. See step 9 in Procedure 30-11.

This completes the summary of essential network commissioning requirements.

SR NE pre-provisioning

7 Configure PW routing:

a using the navigation tree (see Procedure 75-1)

b using the Manage Services form (see Procedure 75-2)

Configure a dynamic MS-PW service

8 Configure a dynamic MS-PW service using PW routing. See Procedure 75-3.

Optional PW routing and MS-Service tasks

9 As required, perform one or more of the following:

a On-demand resync of the MS-PW routing table for a specified NE is supported and can be accessed from a number of places in the 5620 SAM. See Procedure 75-4 for information on displaying MS-PW routing tables.

b Conduct various spoke SDP FEC operations from the endpoint of an Epipe site. See Procedure 75-5.

c Discover and manage MS-PW switching sites. See Procedure 75-6.

d Run an OAM VCCV Ping or Trace validation test for the MS-PW service. See Procedure 75-7.

75.3 PW routing and dynamic MS-PW service management procedures

This section contains the configuration and management procedures required to configure PW routing and dynamic MS-PW services using the 5620 SAM.

Procedure 75-1 To configure PW routing using the navigation tree

This procedure creates service routes for the MS-PW routing on the NE using the navigation tree. Configuration of the following steps is required on the T-PE or S-PE, as detailed.

1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

2 Click on the Globals tab and then the Service sub-tab.

3 Click on the PW Routing sub-tab and then its General sub-tab.

4 Configure the parameters:

- SPE Address
- Boot Timer (seconds)
- Retry Timer (seconds)
- Retry Count

The SPE Address must be unique in the network. This parameter must be configured on all T-PEs and S-PEs that are involved in this PW routing.

The Number of BGP Routes, Number of Static Routes, Number of Local Routes, and Number of Host Routes attributes are for information only and can be resync-ed from the NE.

5 Click on the Local Prefixes sub-tab under PW Routing.

6 Click the Create button. The PW Routing NE Local Prefix (Create) form opens.

7 Configure the Local Prefix parameter.

You must configure this parameter to enable the MS-PW routing configuration on a T-PE node. This Local Prefix is also used in other portions of the MS-PW configuration, such as setting static routes on the remote T-PE or intermediate S-PEs, and setting Source Attachment Individual Identifier (SAII) and Target Attachment Individual Identifier (TAII) addresses on a spoke SDP FEC on the T-PE.

8 Click the Create button in the BGP RD block. The PW Routing NE BGP RD (Create) form opens.

A route distinguisher must be configured to enable this local prefix to be advertised by MP-BGP to the network.

9 Configure the Route Distinguisher parameter.

10 Click the Select button to configure the BGP Community parameter.

The Community can only be selected from the list. Members were created as part of the routing policy configuration in Procedure 30-11 and importing the routing policy under the BGP site in Procedure 31-2.

11 Click on OK.

12 Repeat steps 8 to 11 to create up to four route distinguishers per local prefix.

13 Repeat steps 5 to 13 to create up to 16 local prefixes per NE. The local prefixes you create must be unique in the network.

14 Click the OK button. The PW Routing NE Local Prefix (Create) form closes.

At this point the NE can start to advertise the defined local prefix to its BGP peers.

15 Click on the Static Routes sub-tab under PW Routing.

16 Click the Create button. The PW Routing NE Static Route Configuration (Create) form opens.

A static route can be configured on both the T-PE and S-PE, based on your requirements.

17 Click the Select button to configure the Target T-PE’s PW Address parameter.

This specifies the local prefix defined in the remote T-PE. It can be selected from a managed T-PE or S-PE, or directly entered.

18 Click the Select button to configure the Next Hop parameter.

This specifies the system IP address of the next-hop S-PE or T-PE. It can be selected from a managed T-PE or directly entered.

19 Click the OK button. The PW Routing NE Static Route Configuration (Create) form closes.

At this point the NE can start to advertise the defined static route to its BGP peers.

20 Click on the Configured Paths sub-tab under PW Routing if you need to configure an explicit path. All such configured paths are displayed in the list.

The path should be configured on the T-PEs, which is then used in the spoke SDP FEC to establish a pseudo-wire through the specified path.

21 Click the Create button. The PW Routing NE Path Configuration (Create) form opens, with the General tab displayed.

22 Specify a Path Name.

23 Click the Create button in the Hops block. The PW Routing Hop (Create) form opens.

24 Configure the Hop ID parameter.

25 Configure the Hop Address parameter.

This specifies the system IP address of the next-hop S-PE or T-PE (where the T-LDP session to a given S-PE terminates). It can be entered directly or chosen from the managed S-PE or T-PE by clicking the Select button.

26 Click the OK button. The PW Routing Hop (Create) form closes.

27 Repeat steps 23 to 26 to create the required hops.

28 Click the OK button. The PW Routing NE Path Configuration (Create) form closes.

Procedure 75-2 To create, modify, or view a PW routing NE configuration using the Manage Services form

Perform this procedure to create, modify, or view a PW Routing NE configuration using the Manage PW Routing NE Configuration form. This is an alternative approach to the SR NE pre-provisioning section detailed in the procedural workflow in Procedure 75-1.

1 Choose Manage→Service→PW Routing NE Configuration from the 5620 SAM main menu. The Manage PW Routing NE Configuration form opens.

2 Configure the drop-down filter criteria for PW Routing NE Path Configuration and click the Search button. A list of PW Routing NE configurations appears in the form.

3 Choose the required PW Routing NE configuration and click on the Properties button. The PW Routing NE Configuration (Edit) form opens with the General tab displayed.

4 Configure the parameters, as required:

- SPE Address
- Boot Timer (seconds)
- Retry Timer (seconds)
- Retry Count

5 Click the Local Prefixes tab.

6 Click the Search button and then Properties for an existing prefix, or the Create button for a new one from this tab. If you are creating a new local prefix, configure the Local Prefix parameter on the General tab of the PW Routing NE Local Prefix form.

Whether you are working with an existing or a new local prefix, you can also search for or create new BGP RDs for the current prefix.

7 Click the Search button and then Properties for an existing BGP RD, or the Create button for a new one from this tab. If you are creating a new BGP RD, configure the Route Distinguisher and Community parameters in the PW Routing NE BGP RD (Create) form.

8 Click OK to close the PW Routing NE BGP RD (Create) form. The new BGP RD appears in the list.

9 If there are local spoke SDP FECs associated with this local prefix, click the Local Spoke SDP FECs tab to list them. Select an item from the list and click Properties to view the object information, if required.

10 Click the Static Routes tab.

11 Click the Search button and then Properties for an existing static route, or the Create button for a new one from this tab. If you are creating a static route, configure the Target T-PE's PW Address and Next Hop parameters in the PW Routing NE Static Route Configuration (Create) form.

12 Click OK to close the PW Routing NE Static Route Configuration (Create) form. The new static route appears in the list.

13 Click the Configured Paths tab.

14 Click the Search button and then Properties for an existing path configuration, or the Create button for a new one from this tab. If you are creating a new path configuration, configure the Path Name parameter on the General tab of the PW Routing NE Path Configuration form.

Whether you are working with an existing or a new path configuration, you can also search for or create new Hops for the current configuration.

15 Click the Search button and then Properties for an existing Hop, or the Create button for a new one from this tab. If you are creating a new Hop, configure the Hop ID and Hop Address parameters in the PW Routing Hop (Create) form.

16 Click OK to close the PW Routing Hop (Create) form. The new Hop appears in the list.

17 If there are spoke SDP FECs associated with this path configuration, click the Spoke SDP FECs tab to list them. Select an item from the list and click Properties to view the object information, if required.

18 Click OK to close PW Routing NE Configuration (Edit) form.

Procedure 75-3 To configure a dynamic MS-PW service using PW routing

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria for Service→VLL (VLL)→Epipe Service→(Epipe). A list of services appears at the bottom of the Manage Services form.

3 Choose the required VLL Epipe service that contains the T-PE site and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

4 Click on the Spoke SDP FECs tab.

5 Click the Create button. The Spoke SDP FEC (Create) form opens.

Note — Only one spoke can be configured on the terminating site, including both regular spoke SDP bindings and spoke SDP FECs.

6 Configure the parameters:

- PW ID
- Auto-Assign ID
- SAII Address
- SAII AC ID
- Auto Config
- TAII Address
- TAII AC ID
- Administrative State
- Signaling Type
- Retry Timer (seconds)
- Retry Count
- Path
- PW Template

The Auto Config parameter enables automatic endpoint configuration. This allows the configuration of a spoke SDP endpoint without specifying the TAII associated with that spoke SDP. In this mode, the far end T-PE actively initiates MS-PW signaling and will send the initial label mapping message using T-LDP, while the T-PE for which Auto Config is specified will act as the passive T-PE. The Auto Config parameter cannot be enabled if the Signaling Type is set to Master or if the TAII Address is specified.

If you are going to use SAII and TAII addresses instead of Auto Config, then you must decide which method will be used for the PW routing.

- For dynamic PW routing, the local prefix associated with the SAII/TAII address should be configured with a route distinguisher, with an optional community (refer to steps 8 to 12 in Procedure 75-1). The SAII and TAII addresses must be unique in the network.
- For static routing, the local prefix should be associated with static routes configured under PW routing (refer to steps 15 to 19 in Procedure 75-1). A spoke SDP FEC cannot be turned up if no local prefix is configured under PW routing.
- When using a specified path, the Path parameter must be configured. The associated Select button allows you to select a path that will be used for this spoke SDP and which is configured under PW Routing. If no path is configured, then each next hop of the MS-PW used by the spoke SDP will be chosen locally at each S-PE and T-PE, using dynamic PW routing.

7 If redundancy is required, specify an Endpoint using the associated Select button.

8 Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State
- Enable PW Standby Signaling Slave

9 Click the Return Spoke SDP FEC tab to configure a return spoke SDP FEC, as required.

This tab is only displayed when the TAII Address configured in step 6 was set by selection for the current spoke SDP FEC.

10 Configure the PW ID parameter for the return spoke SDP FEC and click Apply.

When a valid PW ID for the return spoke SDP FEC is entered, additional parameters are displayed. If the PW ID is not valid, then the return spoke SDP FEC will not be created.

11 Configure the parameters:

- Signaling Type
- Auto Config
- Path
- PW Template
- Set ICB

12 Specify an Endpoint using the associated Select button.

When the return spoke SDP FEC is created, it will have corresponding attributes such as the SAII and TAII Address values and AC ID cross-matching with the current spoke SDP FEC.

13 Click OK to apply the configurations and close the Spoke SDP FEC (Create) form.

When a spoke SDP FEC is successfully created, it will be listed under the Spoke SDP FECs tab for this Epipe site.

14 Select the spoke SDP FEC from the list and click Properties.

The spoke SDP FEC should contain the following tabs: General, Spoke SDP Associated, Tests, and Faults.

The Spoke SDP Associated tab will list the spoke SDP bindings created by using this Spoke SDP FEC for MS-PW routing. All such spoke SDP bindings have their Creation Mode attribute set as Multi-Segment PW. The related SDP FEC Auto-bind tab shows the associated SAII or TAII defined in the Spoke SDP FEC.

The Faults tab will display any mis-configuration alarms associated with this spoke SDP FEC.

15 Close the Epipe Service (Edit) form.

When the configuration for both T-PEs is complete, the NEs can start negotiating and establishing the spoke SDP bindings from T-PE to S-PE and from S-PE to T-PE.

Procedure 75-4 To display MS-PW routing tables

On-demand resync of the MS-PW routing table for a specified NE is supported and can be accessed from a number of places in the 5620 SAM.

1 Select an applicable NE from one of the following locations:

- Navigation tree
- Physical Topology map
- Service Tunnel map

2 Right-click the NE to open the pop-up menu.

3 Click on the Show MS-PW Routes and select one of the following show commands:

- BGP
- Service

The Service Routing rtr BGP or Service Routing rtr Service form opens accordingly. The requested routing table information is presented, along with a detailed status/error report.

4 Close the Service Routing rtr report form.

Procedure 75-5 To perform spoke SDP FEC operations from an endpoint

Perform this procedure to conduct various spoke SDP FEC operations from the endpoint of an Epipe site.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2. Configure the filter criteria for Service→VLL (VLL)→Epipe Service→(Epipe). A list of services appears at the bottom of the Manage Services form.

3. Choose the required VLL Epipe service that contains the primary and backup spoke SDP FECs and click on the Properties button. The Epipe Service (Edit) form opens with the General tab displayed.

4. Expand the Spoke SDP FECs item under the required Epipe site in the navigation tree.

5. Right-click the required Spoke SDP FEC. A pop-up menu appears. Select the required action:

    - Force Switchover
    - Clear Forced Switchover
    - Turn Up
    - Shut Down
    - Delete
    - Resync
    - Properties

    The Forced Switchover and Clear Forced Switchover options are only applicable where the Epipe site has been configured for redundancy, as detailed in Procedure 75-1. The switchover applies to the primary and backup spoke SDP FECs configured on the Epipe site.

6. Close the Epipe Service (Edit) form.

Procedure 75-6 To discover and manage MS-PW switching sites

With PW routing configured on T-PEs and S-PEs, and spoke SDP FECs configured on the T-PEs, the SR 7x50 will establish the pseudo-wires between T-PEs. This includes creating switching sites between two T-PEs. A switching site for MS-PW is a read-only site (nothing can be modified) and it cannot be deleted. It is controlled by the NE.

Use the following method to discover such sites, if required.

Note 1 — The switching sites and spoke SDP bindings created by MS-PW routing are tagged with their Creation Mode attribute indicating Multi-Segment PW (as opposed to Manual for non-MS-PW entities).

Note 2 — When a switching site is discovered, the associated spoke SDP bindings under it are also discovered and re-synced. The 5620 SAM will create a composite service and connector(s) if there are matching spoke SDP bindings found in other Epipe services (based on cross-matching of the spoke SDP ingress/egress labels). The related service is added to the newly-created composite service.

1 Conduct an RCA Audit to discover switching sites, if required. This is done within the Epipe service that contains the T-PEs having MS-PW configured. The audit will find all MS-PW switching sites associated with T-PEs in this service and provide management solutions.

Refer to Procedure 81-1 for details on configuring an RCA audit.

2 Perform Procedure 81-2.

Procedure 75-7 To conduct MS-PW routing OAM tests

The MS-PW routing configuration can be tested using OAM VCCV Ping and Trace tests.

1 To conduct a VCCV Ping test refer to Procedure 38-23.

The test can be created either from the Service Test Manager or from a configured Epipe service, Epipe site, or a Spoke SDP FEC.

If you choose a spoke SDP binding created by MS-PW routing, the VCCV ping is specifically for MS-PW, and the SAII and TAII parameters will be auto-filled. This allows you to conduct a MS-PW VCCV Ping on an S-PE.

If the test is created from a configured Spoke SDP FEC, the test object will be auto-filled with the configured spoke SDP FEC.

Alternatively, if the test is created from the Service Test Manager, an Epipe service, or an Epipe site (both the termination site and the switching site), then you must select a spoke SDP FEC (only for T-PE) or a spoke SDP binding of type FEC 129 created by the MS-PW routing.

2 To conduct a VCCV Trace test refer to Procedure 38-24.

The test can be created either from the Service Test Manager or from a configured Epipe service, Epipe site, or a Spoke SDP FEC.

If the test is created from a configured Spoke SDP FEC, the test object will be auto-filled with the configured spoke SDP FEC.

Alternatively, if the test is created from the Service Test Manager, an Epipe service, or an Epipe site (both the termination site and the switching site), then you must select a spoke SDP FEC (only for T-PE) or a spoke SDP binding of type FEC 129 created by the MS-PW routing.

Note 1 — When configuring either a VCCV Ping or VCCV Trace test for dynamic MS-PW from an S-PE, the Reply Type must be set to IP.

Note 2 — If the selected spoke SDP binding is created by MS-PW routing, you can only conduct a VCCV ping for MS-PW FEC129, not for FEC128.

Note 3 — If a PW template is used in the Spoke SDP FEC configuration, it must have its Enable Control Word parameter enabled, since both VCCV Ping and Trace require Control Word support.

3 To create a Test Suite refer to Procedures 78-8 and 78-12.

A Test suite can be generated based on the selected policy for a specified VLL Epipe service.

If the selected policy has its Entity Type set to VLL Service, then the VCCV Ping and VCCV Trace tests that are generated will adhere to the following:

- No tests are generated for spoke SDP bindings created by MS-PW routing.
- Both VCCV Ping and VCCV Trace tests for MS-PW will be generated if there are spoke SDP FECs in the specified Epipe service.

If the selected policy has its Entity Type set to Service Connector, then there is also no test generated for the spoke SDP bindings created by MS-PW.

76 — Composite service management

76.1 Composite service management overview

A composite service is a set of linked services. Composite service functionality supports complex applications that require a combination of services, such as VLAN connections to an HVPLS, an IES spoke into a VPLS, or a VPRN-to-VPLS interconnection.

Services that are owned by different customers can be connected to form a composite service. An example is an HVPLS in which the core VPLS belongs to one customer and the satellite VPLS instances belong to other customers. An HVPLS is considered to be a composite service by the 5620 SAM.

Composite services consist of customer services, called SCs in the context of a composite service, and connectors. A connector is a bidirectional logical link between two SCs, such as a pair of PW spokes that carry traffic in opposite directions between VLL and VPLS instances, a dot1q-encapsulated link between a VLAN and a VPLS, or an internal cross-connect.

The term SCP describes a type of connector endpoint. In the case of the services that are available on the 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, or the 7750 SR, an SCP is a service interface or SAP. For L2 switches, such as the 7250 SAS or Telco, an SCP may be a network interface, such as an uplink port.

Composite services exist only in the context of the 5620 SAM and are configured through the 5620 SAM GUI or an OSS application. They are unknown to individual network devices. To simplify composite service configuration and to ensure that non-5620 SAM device configuration does not disrupt the management of composite services, the following rules apply to the creation, deletion, modification, and presentation of composite services.

- A composite service can have zero SCs.
- A composite service can have zero connectors.
- Two connected SCs can belong to only one composite service.
- A connector between two SCs belongs to only one composite service.
- An SC cannot be removed from a composite service until its connector to the composite service is removed.
- A group of connected services can be moved from one composite service to another.

The 5620 SAM supports composite-service configuration using the following methods.

- Tabbed configuration forms with an embedded navigation tree that provides a logical, hierarchical view of the composite service and acts as a configuration interface. When you right-click on an object in the navigation tree, a menu specific to the object appears. When you choose an object in the menu, the related configuration form opens.
- Connector creation and configuration from within the composite service's flat topology view
- Pre-configured template. A user that is assigned the service management scope of command role can create a composite-service template. The service management user can also create a connector template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with creating and using templates.

If a service that is specified for inclusion in a composite service does not currently belong to a composite service, it is added to the composite service regardless of its administrative or operational state. If the specified service is part of an existing composite service, it can be moved to a different composite service. However, SCs that are connected to the specified service are also moved to the new composite service upon confirmation of the action by the 5620 SAM operator. The 5620 SAM performs no such action confirmation for OSS applications.

When services within a composite service have the same service ID, the 5620 SAM raises an alarm. For example, a VPLS with service ID 5 on one NE and an IES service with service ID 5 on another NE are combined to create a composite service. The operational status of the composite service is up and the composite service functions correctly, however, an alarm is raised because the 5620 SAM does not support the configuration of two services using the same service ID. This situation may arise when services are created on NEs using a CLI rather than through the 5620 SAM.

Hierarchical organization of composite services

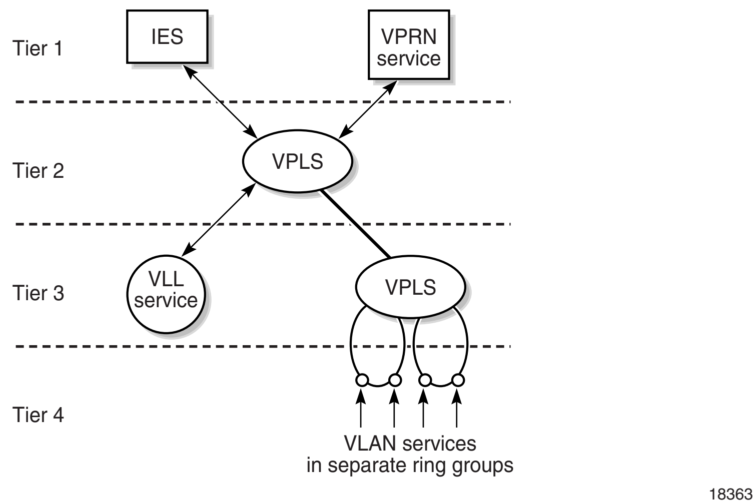
The 5620 SAM organizes the SCs in a composite service by tiers within a hierarchy during network discovery and for display purposes. When you add an SC to a composite service, the 5620 SAM assigns a default tier value to the SC according to the service type. Table 76-1 lists the default tiers for different service types.

Table 76-1 Default tiers for service types

Service type	Default tier
IES and VPRN	1
VPLS and MVPLS	2
VLL	3
VLAN	4

The default tier values reflect common deployment configurations. Figure 76-1 shows a composite service hierarchy. SCs are not restricted to the default tiers, as in the case of the VPLS in Tier 3 that forms an HVPLS with the VPLS in Tier 2.

Figure 76-1 Default SC tier assignments



You can change the tier of an SC at any time and can specify a value other than one of the defaults that the 5620 SAM assigns; composite services can have many tiers.

The tier value of an SC determines the relative position of the SC within a composite service topology map. The 5620 SAM displays SCs in rows by tier, in numerical order from the top of the panel downward, beginning with tier 1.

You can move SC icons in a composite service topology map from one tier to another for a customized view, then use the Rearrange by Service Tiers button to organize the SC icons in the map panel according to tier.

Caution — The composite service topology map is redrawn when you click on the Rearrange by Service Tiers button, and you cannot revert to the former layout of the composite service topology map.

See chapter 5 for more information about 5620 SAM map management.

Network discovery of composite services

The 5620 SAM associates SCs and connectors with composite services during network discovery. The following rules apply to this process.

- When the 5620 SAM discovers a valid connector between two services that do not belong to a composite service, a composite service that contains the services and connector is automatically created.
- When the 5620 SAM discovers a valid connector between two services and one of the services belongs to a composite service, the other service is added as an SC of the composite service.
- When the 5620 SAM discovers a valid connector between two services and the two services are SCs of different composite services, an alarm is raised and the connector is excluded from the 5620 SAM database.

The 5620 SAM assigns a default tier value to a service upon creation and to a new SC during network discovery. The tiered hierarchy provides a common framework for service configurations that are provisioned through the 5620 SAM and CLI. A 5620 SAM operator can assign a different tier value to an SC after discovery.

A composite service has Aggregated Operational State, Connection State, and Service Component Degraded status indicators. The General tab of the Composite Service management form displays these indicators.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the aggregated SC operational states as follows.

- Up—All SCs are operationally up
- Partially Down—At least one SC is operationally down
- Down—All SCs are operationally down
- Unknown—The status of at least one SC is undetermined

The Connection State indicator displays one of three values, as follows:

- No Connection—None of the SCs is connected to any other SC
- Partially Connected—One SC is not able to communicate directly or indirectly with all other SCs
- Strongly Connected—All SCs are able to communicate

For example, a composite service has five services named A, B, C, D, and E. A is connected to B, C is connected to D, and D is connected to E. The Connection State in this case is Partially Connected. When A or B becomes connected to C, D, or E, the Connection State becomes Strongly Connected.

The Service Component Degraded indicator shows whether there is an operational flag set on any of the service sites under this composite service.

Connector types

The following types of connectors join SCs in a composite service:

- SCP-to-SCP
- internal cross-connect
- PW spoke
- routed VPLS

SCP-to-SCP connectors

SCP-to-SCP connectors can join any two SC types that have service interfaces on the same device or on different devices. A connector between VPLS and VPRN SAPs is an SCP-to-SCP connector, as is a connector between a dot1q-encapsulated VPLS SAP and L2 switch uplink port in a VLAN ring group. Table 76-2 describes the supported encapsulation types.

Table 76-2 Supported encapsulation types

SAP type	Encapsulation type
Ethernet	dot1q
	Q in Q
	Null
ATM	VPI/VCI
	VPI
FR	DLCI
SONET/SDH	BCP Null
	BCP dot1q
	IPCP
	PPP Auto
	cHDLC
	WAN Mirror
LAG	Null
	dot1q

The operational status of an SCP-to-SCP connector depends on the operational status of its endpoints. An alarm raised against one of the endpoints causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Internal cross-connect connectors

An internal cross-connect connector can join any SC types. It uses a CCAG to join two SCs that have SAPs or network interfaces on the same device. This functionality is available in the 7450 ESS, 7710 SR, and 7750 SR. The following rules apply to internal cross-connect connectors.

- A SAP can be connected to another SAP or to a network interface using a CCAG.
- When a SAP or network interface is deleted, the connector associated with it is also deleted.
- The deletion of an internal cross-connect connector causes the associated interfaces and SAPs to be deleted.

The operational state of an internal cross-connect connector depends on the operational state of the CCAG. An alarm raised against the CCAG causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

PW spoke connectors

A PW spoke connector generally joins VPLS instances to create an HVPLS. In the 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7750 SR, a PW spoke can, for example, connect IES and VPLS instances to provide distributed Internet access service. The endpoints of a PW spoke connector must be on different devices. PW spoke connectors are subject to restrictions on the SC types that they can join. Table 76-3 shows the SC types that can be linked by PW spoke connectors.

Table 76-3 Valid PW spoke interconnections

SC type	Valid PW spoke SC interconnections
VLL	IES, VPLS
VLAN	—
VPLS	IES, VLL, VPLS
MVPLS	MVPLS
IES	VLL, VPLS
VPRN	VLL, VPLS

The operational state of a PW spoke connector depends on the operational state of the underlying SDP bindings. An alarm raised against one of the SDP bindings causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Routed VPLS connectors

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. Although an IES or VPRN IP interface can only be bound to a single VPLS site, the service context that contains the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the binding depends on the operational state of the VPLS site, or whether the IP interface binding is enabled on the VPLS site.

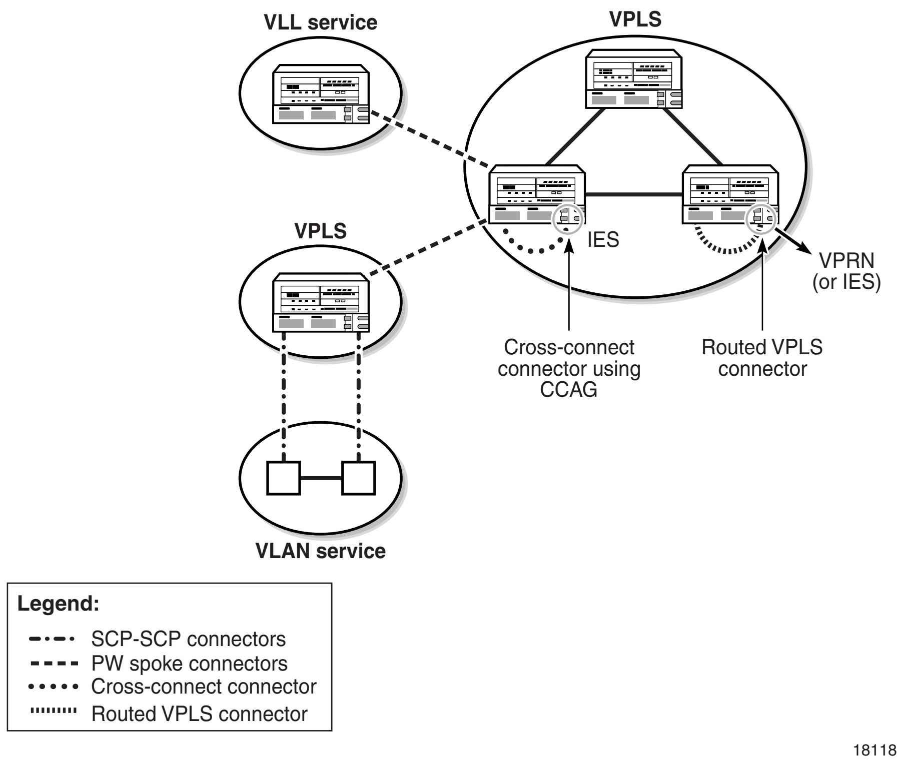
The operational state of the routed VPLS connector depends on the operational state of the binding and the operational state of the L3 IP interface.

The routed VPLS connector function is supported for IOM3 cards in a Release 8.0R4 or later 7450 ESS in mixed mode, a Release 8.0R4 or later 7750 SR, or a Release 8.0R5 or later 7750 SR-c4.

76.2 Sample composite service configuration

Figure 76-2 shows a sample composite service configuration that involves a variety of customer services and uses the three SC connector types.

Figure 76-2 Sample composite service configuration



76.3 Workflow to create a composite service

The following workflow lists the high-level steps required to create a composite service. As a prerequisite for creating a composite service, this workflow assumes the following:

- a group or customer with the required user access privileges has been set up; see chapter 9 for more information.
- the IP or IP/MPLS core network exists.
- any required service tunnels are created including the static or dynamic LSP required to create the service tunnel; see Procedure 33-1 for more information.
- the access ports for the service are created; see chapter 20 for more information.
- any required pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies are created; see chapter 46 for more information. You do not have to create pre-defined policies if policies are created on a per-service basis.

- any required MP-BGP for PE-to-PE routing is configured; see chapter 31 for more information about protocol configuration.
- the other network services that are to be the SCs of the composite service are created.

1 Create the composite service. See Procedure 76-1 for more information.

  i Define the general properties for the composite service.

  ii Specify the services for inclusion in the composite service. You can specify multiple services in one operation.

  iii Create connectors to link the SCs of the composite service.

  iv Turn up the composite service.

2 View the service topology map associated with a composite service. See Procedure 76-2 for more information.

3 As required, run an OAM validation test for a composite service. See Procedure 76-3 for more information.

4 As required, modify a composite service:

  a using the navigation tree; see Procedure 76-4 for more information

  b using the flat topology view; see Procedure 76-5 for more information

5 As required, delete a composite service. See Procedure 76-6 for more information.

76.4 Composite service management procedures

Use the following procedures to perform composite service creation and management tasks.

Procedure 76-1 To create a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Click on the Create button. The Composite Service (Create) form opens.

3 Configure the parameters.

- Composite ID
- Auto-Assign ID
- Name
- Description

4 Click on the Apply button. The form title changes to Composite Service *Service Name* (Edit) and the form displays an additional tab button and Status and OLC panels.

5 Configure the OLC State parameter.

6 Perform one of the following:

a Add an SC to the composite service. Go to step 7.

b Complete composite service creation if SCs and connectors are to be added later. Go to step 18.

7 In the navigation tree, right-click on the Services icon and choose Add Services. The Add Services form opens.

Note — You can also create a service for inclusion in the composite service by right-clicking on the Services icon and choosing Create *Service Type*.

8 Click on the Search button. A list of available services is displayed.

9 Select a service and click on the OK button. You can select multiple services. The CompositeService - *Service Name* (Edit) form refreshes with the SC information displayed.

10 Perform one of the following:

a Add a connector to the composite service. Go to step 11.

b Complete composite service creation if connectors are to be created later. Go to step 18.

11 Right-click on the Connector icon in the navigation tree and choose one of the following options:

a Create CrossConnect. Go to step 12.

b Create RoutedVplsConnector. Go to step 13.

c Create ScpConnector. Go to step 14.

d Create SpokeConnector. Go to step 15.

12 The Cross Connect (Create) form opens.

Note — The service endpoints of a cross-connect connector must be on the same NE.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Cross Connect form opens with a list of available SCs displayed.

iii Choose an SC and click on the OK button. The Select Service A - Cross Connect form closes and the Cross Connect (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Cross Connect form opens with a list of available SCs displayed.

v Choose an SC and click on the OK button. The Select Service B - Cross Connect form closes and the Cross Connect (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

vii Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose an SC to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

ix Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

x Click on the Transport tab button.

xi Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

xii Choose a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the Cross Connect (Create) form refreshes.

xiii Configure the parameters.

- CC ID
- Auto-Assign ID

xiv Click on the OK button. The Cross Connect (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xv Go to step 17.

13 The RoutedVplsConnector (Create) form opens.

i Configure the parameters:

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - RoutedVplsConnector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - RoutedVplsConnector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

Note — The sites that you select in substeps vii and ix must be located on the same NE.

x Click on the Routed-VPLS L3 Connection Point tab button.

xi Click on the Select button to choose an interface for the connector. The Select L3 Access Interface - RoutedVplsConnector form opens with a list of available L3 Access Interfaces displayed.

xii Select an L3 Access Interface and click on the OK button. The RoutedVplsConnector (Create) form refreshes.

xiii Click on the OK button. The RoutedVplsConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xiv Go to step 17.

14 The ScpConnector (Create) form opens.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - ScpConnector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - ScpConnector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - Scp Connector form closes and the ScpConnector (Create) form refreshes.

x Click on the Service Connection Point tab button.

xi Click on the Select button in the Service Connection Point A panel to choose an SCP to associate with the connector. The Select Service Connection Point A - Scp Connector form opens with a list of available SCPs displayed.

xii Select an SCP and click on the OK button. The Select Service Connection Point A - Scp Connector form closes and the ScpConnector (Create) form refreshes.

xiii Click on the Select button in the Service Connection Point B panel to choose an SCP to associate with the connector. The Select Service Connection Point B - Scp Connector form opens with a list of available SCPs displayed.

xiv Select an SCP and click on the OK button. The Select Service Connection Point B - Scp Connector form closes and the ScpConnector (Create) form refreshes.

xv Click on the OK button. the ScpConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xvi Go to step 17.

15 The SpokeConnector (Create) form opens.

Note — The service endpoints of a spoke connector must be on different NEs.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Spoke Connector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Spoke Connector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site from service A to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site from service B to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

x Click on the Transport tab button.

xi Configure the parameters.

- VC ID
- Auto-Assign ID
- Auto Select Tunnels
- Transport Type

The Transport Type parameter is configurable when the Auto Select Tunnels parameter is enabled.

xii If the Auto Select Tunnels parameter is enabled, go to step xvii.

xiii Click on the Select button in the Tunnel A panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site A - Spoke Connector form opens with a list of available service tunnels displayed.

xiv Select a tunnel and click on the OK button. The Select Tunnel From Site A - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

xv Click on the Select button in the Tunnel B panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site B - Spoke Connector (Create) form opens with a list of available service tunnels displayed.

xvi Select a tunnel and click on the OK button. The Select Tunnel From Site B - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

xvii The First L3 Access Interface panel is present, if one of the SCs in the composite service is an IES. If the First L3 Access Interface panel is not present, go to step xxii.

xviii Click on the Select button in the First L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select First L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

xix The Second L3 Access Interface panel is present, if another of the SCs in the composite service is an IES. If the Second L3 Access Interface panel is not present, go to step xxii.

xx Click on the Select button in the Second L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select Second L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

xxi Select an L3 access interface and click on the OK button. The Select L3 Access Interface - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

xxii Click on the OK button. The SpokeConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

16 Configure alarm aggregation for the composite service components, if required.

i Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens.

ii Enable the Alarm Aggregation to Composite Service parameter.

iii Click OK. A confirmation window is displayed.

iv Click Yes. The System Preferences form closes.

17 Perform one of the following:

a Add an SC to the composite service. Repeat steps 7 to 9.

b Add a connector to the composite service. Go to step 11.

c Complete site creation. Go to step 18.

18 Click on the OK button. The CompositeService - *Service Name* (Edit) form closes and a dialog box appears.

19 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

20 Close the Manage Composite Services form.

Procedure 76-2 To view the service topology map associated with a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and perform one of the following steps:

  a Click on the Topology View button. A Composite Service Topology - *Service Name* map opens.

  b Click on the Topology View Flat button. A Composite Service Flat Topology - *Service Name* map opens. The Flat Topology map is a flattened view of a composite service, meaning that all the service objects are displayed simultaneously, along with the service sites, access interfaces, and the links or groups of links between them.

  See chapter 5 for more information about composite service topology views.

Procedure 76-3 To run an OAM validation test for a composite service

A validator test suite must be created for the tested entity. See chapter 78 for more information about how to create a validator test suite.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria and click Search. A list of composite services appears in the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The Composite Service (Edit) form opens with the General tab displayed.

4 Click on the Action button and select Validate. If a validator test suite is not associated to the composite service, a dialog box appears. Perform the following steps:

  i Click on the OK button to associate the composite service with an existing validator test suite. The Choose Validator Test Suite form appears.

  ii Configure the filter criteria. A list of validator test suites appears.

  iii Select a validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the Operational Flags indicators. If the validation test fails, a check mark appears beside the OAM Validation Failed indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the Composite Service (Edit) form.

11 Close the Manage Composite Services form.

Procedure 76-4 To modify a composite service using the navigation tree

Caution — Modifying parameters can be service-affecting.

Note — You can also modify composite service components and add service connectors from the flat topology view. Refer to Procedure 76-5.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 To configure parameters for an item, in the navigation tree, select and right-click on the item, and choose Properties from the contextual menu.

Using the contextual menu, you can also:

- Add SCs and connectors to a composite service
- Create services for inclusion in the composite service. When you create services by using the contextual menu, the services are automatically added to the composite service.
- Remove SCs and connectors from a composite service
- Move SCs to another composite service
- Delete SCs

Warning — Deleting an SC is not the same as removing an SC from a composite service. Deleting an SC removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

7 Click on the Close button to close the Manage Composite Services form.

Procedure 76-5 To modify a composite service using the flat topology view

You can modify composite service components and add service connectors from the flat topology view. The main advantage of creating connectors using the flat topology view is that most of the parameters in the associated configuration forms are automatically populated when you select an item in the map.

Caution — Modifying parameters can be service-affecting.

Note — You can also modify and add composite service components using the navigation tree. Refer to Procedure 76-4.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 Click the Flat Topology View button. The Composite Service Flat Topology map opens.

5 To configure parameters for any item on the map, right-click on the item, and choose Properties from the contextual menu. The configuration form for the item is displayed.

6 Edit the parameters as required. Refer to Procedure 76-1 for detailed configuration information on creating and configuring components.

7 Add service connectors to the composite service, if required.

Depending on the sites or ports you select, when you right-click on a component, the contextual menu contains one or more of the following choices:

- Create Cross Connect. Go to step 8.
- Create Routed Vpls Connector. Go to step 9.
- Create Scp Connector. Go to step 10.
- Create Spoke Connector. Go to step 11.

Click on the required item in the contextual menu and proceed to the associated step indicated in this list.

Note — If you need to modify any of the automatically-populated parameters in the associated configuration forms while creating these connectors, refer to Procedure 76-4 for detailed information.

8 To create a Cross Connect Connector:

i Select the two site icons that you want to create the Cross Connect Connector for. These icons represent the same physical NE that exists in two separate services, since service endpoints of a Cross Connect Connector must be on the same NE.

ii Right-click on either of the icons and select Create Cross Connect from the contextual menu.

The CrossConnect (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the Transport tab button.

v Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

vi Select a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the CrossConnect (Create) form refreshes.

vii Click on the OK button. The CrossConnect (Create) form closes and the new Cross Connect Connector is displayed on the map.

viii Go to step 15.

9 To create a Routed Vpls Connector:

i Select a VPLS site icon and an L3 Access Interface icon that you want to create the Routed Vpls Connector for. These icons must belong to the same NE.

ii Right-click on either of the icons and select Create Routed Vpls Connector from the contextual menu.

The RoutedVplsConnector (Create) form opens with the General tab displayed.

iii Configure the parameters.

- Name
- Description (optional)

- **iv** Click on the OK button. The RoutedVplsConnector (Create) form closes and the new Routed Vpls Connector is displayed on the map.
- **v** Go to step 15.

10 To create a Scp Connector:

- **i** Select the port icons for the two sites that you want to create the Scp Connector for.
- **ii** Right-click on either of the icons and select Create Scp Connector from the contextual menu.

  The ScpConnector (Create) form opens with the General tab displayed.
- **iii** Configure the parameters.
  - Name
  - Description (optional)
- **iv** Click on the OK button. The ScpConnector (Create) form closes and the new Scp Connector is displayed on the map.
- **v** Go to step 15.

11 To create a Spoke Connector:

- **i** Select the two site icons that you want to create the Spoke Connector for. These icons must be two different NEs that exist in two separate services.
- **ii** Right-click on either of the icons and select Create Spoke Connector from the contextual menu.

  The SpokeConnector (Create) form opens with the General tab displayed.
- **iii** Configure the parameters.
  - Name
  - Description (optional)
- **iv** Click on the OK button. The SpokeConnector (Create) form closes and the new Spoke Connector is displayed on the map.

12 Create new services within the composite service view, if required.

- **i** Right-click on the flat topology map background and choose Create from the menu. A list of services appears.
- **ii** Click on the service type you want to create. The appropriate Service (Create) form appears.
- **iii** Configure the parameters for the service as required and then click on the OK button in the Service (Create) form.

See the appropriate service management chapter for information about creating a specific service type.

iv The Service (Create) form closes and the new service is displayed on the map.

13 Add services to the composite service, if required.

i Right-click on the flat topology map background and choose Add→Service(s) from the menu. An Add Services - Composite Services form appears.

ii Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Add Services - Composite Services form.

iii Select a service and click on the OK button. The Add Services - Composite Services form closes and the service is displayed on the map. If the service includes service sites, the sites are also displayed on the map.

14 Add service sites to an existing service in the composite service, if required.

i Right-click on the flat topology map background and choose Add→Service Site(s) from the menu. A Find Service form appears.

ii Configure the filter criteria and click on the Search button. A list of services that are already part of the composite service appears at the bottom of the Find Service form.

iii Select a service and click on the OK button. The Find Service form closes and a Select Network Elements form appears with a list of available NEs.

iv Select one or more NEs and then click on the OK button. A Service Site (Create) form appears. If more than one NE is selected, a Service Site, Multiple Instances (Create) form appears.

v Configure the service site and click on the OK button. The new service site is displayed on the map.

See the appropriate service management chapter for information about configuring a specific service site type.

15 Click on the OK button in the CompositeService - *Service Name* (Edit) form. A dialog box appears.

16 Click on the Yes button to confirm your changes. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

17 Click on the Close button to close the Manage Composite Services form.

Procedure 76-6 To delete a composite service

Warning — Deleting a service may result in a service disruption for customers. Consider the implication of deleting the service before proceeding.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 As required, configure the filter criteria to locate the service or range of services to be deleted. A list of services appears at the bottom of the Manage Services form.

3 Choose a service or a range of services from the list.

4 Click on the Delete button. A warning form appears. This form is dynamic based on the priority of the service. Perform one of the following:

   a For services with a low priority, go to Step 5.

   b For services with a medium priority, configure the "Enter the highest priority of the service being deleted" text field by typing: Medium. Go to Step 5.

   c For services with a high priority, configure the "Enter the highest priority of the service being deleted" text field by typing: High. Go to step 5.

5 For all services regardless of how their priority is configured, acknowledge the check box that prompts you confirm that you understand the implications of deleting the service.

Note — If you select multiple services with different priorities, you must enter the highest priority level of selected services before you can delete the services.

6 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

7 Click on the Close button to close the Manage Services form.

77 — Application assurance

77.1 Application assurance overview

Application Assurance, or AA, is a service-enabling technology that is available for the 7450 ESS and 7750 SR. This technology enhances the existing hierarchical per-subscriber, per-service, and per-application QoS capabilities with granular, per-AQP control. In addition to QoS capability enhancement, AA provides traffic divert, application identification, and statistics collection.

AA can be introduced in existing deployments of the Alcatel-Lucent TPSDA to evolve the HSI legacy into an EIS model that can support bandwidth-intensive Internet-based applications and content delivery.

AA enables deep packet inspection of subscriber traffic where policies are applied to specific types of HSI traffic on a per-subscriber basis to determine the action to perform on the traffic. A subscriber can be associated with one of the following services:

- IES
- VPLS
- VLL
- VPRN

AA and dynamic subscriber policy control allow a broadband network to provide application-based subscriber management for Internet access. The benefits of AA for residential and business service providers are:

- enhanced application-level SLAs through policy-based network traffic controls and improved QoS sophistication at the application and site level
- traffic flow thresholds and threshold crossing notification
- application-aware reporting and performance analysis tools
- complementary security aspects to existing network security
- scalability to support a large number of services, and flexibility to control network costs

The 5620 SAM can manage AA on all 7450 ESS and 7750 SR chassis types except the 7450 ESS-1 and 7750 SR-1.

NE traffic is selected to be processed by AA and then undergoes deep packet inspection on an ISA-AA MDA in the NE. See chapter 18 for information about using the 5620 SAM to configure an ISA-AA group that contains one or more ISA-AA MDAs.

You can configure Cflowd v10 on an ISA-AA group. AA Cflowd supports basic Cflowd sampling as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one Cflowd instance.

You must enable Cflowd globally on an NE before you can configure AA Cflowd collectors. Each collector is deleted when Cflowd is disabled. See chapter 17 for information about enabling and configuring global Cflowd on an NE, and see chapter 18 for information about enabling and configuring AA Cflowd on an ISA-AA group.

Note — AA policies can only be configured on an NE if an ISA-AA group is already configured on the system.

The two elements of AA processing are:

- identification of the traffic on a per-flow or per-session basis
- policy treatment of the identified traffic

Functional components

The 5620 SAM supports the creation and configuration of AA components using configuration forms and scripts.

Figure 77-1 shows the AA functional components.

Figure 77-1 AA functional components

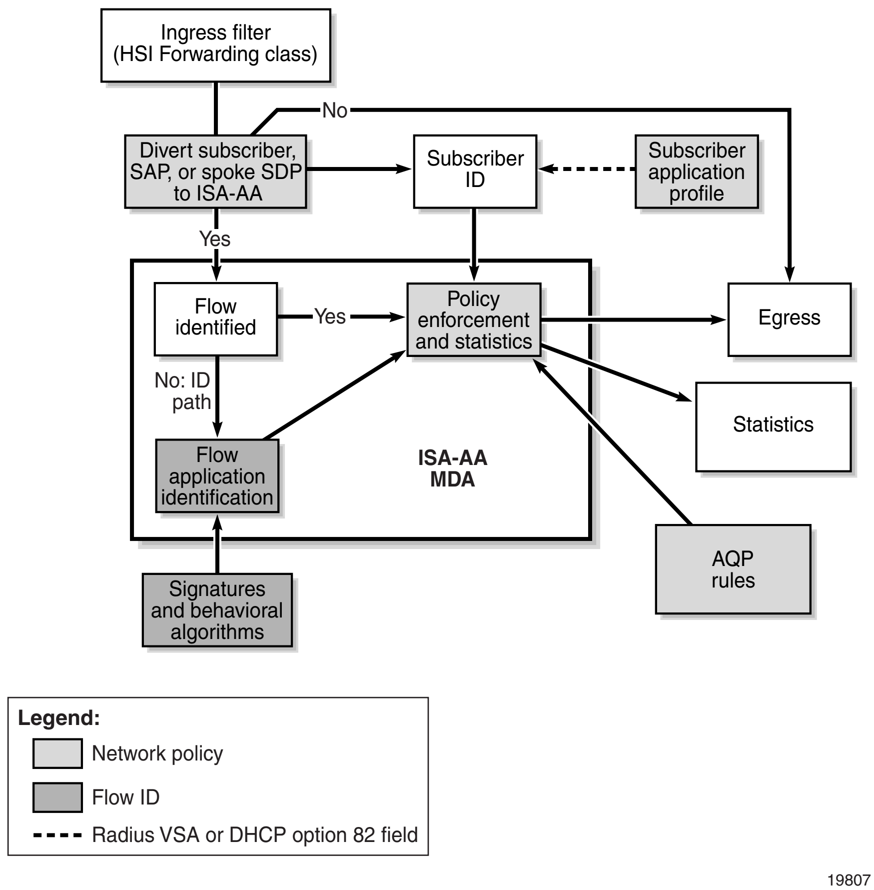
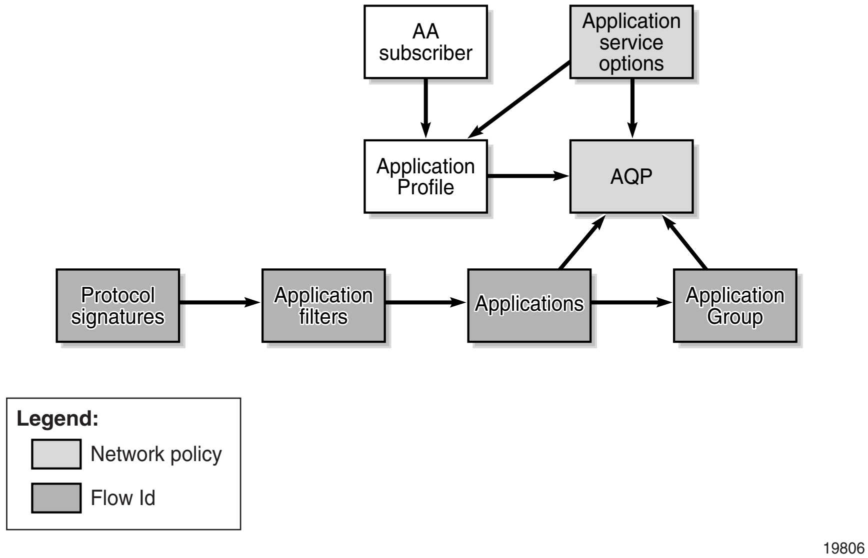


Figure 77-2 shows the relationship between the AA components that are used to identify applications and configure AA-related capabilities.

Figure 77-2 AA policy structure



ISA-AA groups and partitions

The 5620 SAM supports ISA-AA partitions. An ISA-AA partition is a unique child object of an ISA-AA group that can be assigned its own AA policy. There is no relationship between partitions of different ISA-AA groups. You can partition an ISA-AA group into AA policy partitions with one partition for each VPN-specific AA service. The partition supports VPN-specific custom protocols, applications, application group definitions, policy definitions and reporting. Each partition policy can be divided into multiple application QoS policies using ASOs. Multiple ISA-AA groups are used to scale the number of VPN-specific AA policies.

Multiple ISA-AA groups

The following operations can be performed at the ISA-AA group level

- Define one or more ISA-AA groups to allow AA resource partitioning and reservation of different types of AA service.
- Assign physical ISA-AAs to a group.
- Specify forwarding classes to be diverted for inspection by the AA subscribers that belong to the group and choose the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs that host ISA-AA traffic.
- Configure ISA capacity planning using low and high thresholds.
- Enable ISA-AA partitions for ISA-AA groups.

Residential services are an example where all AA services can be configured as part of a single group that encompasses all ISA-AAs. The configuration provides the management of common applications and reporting for all subscribers and services, with common or per-customer AQP (uses ASO characteristics to divide the AQP of the ISA-AA into per-application profile QoS policies).

Multiple ISA-AA groups can also be used to create separate services based on different sets of common applications, traffic diversion needs, or different redundancy models. Multiple ISA-AA groups can be used for:

- a mix of residential and business customers
- different business VPN verticals
- business services with a common template base but different levels of redundancy, forwarding class diversion, or scaling over what is supported per single group

ISA-AA partitions

ISA-AA groups and partitions improve the scaling of policies. If partitions are not configured, the ISA-AA group acts as a single partition. When partitions are configured, application identification, and policy and statistics configuration apply only to the partition and not any other partitions that are configured under the same AA group. Although the definition of application profiles and related ASO characteristics is in the context of a partition, the application profile names must be unique for the NE. Definition of applications, application groups, and AQPs are also specific and only apply to a specific partition.

The following operations can be performed at the ISA-AA partition level

- Define unique applications and application groups per partition.
- Define AQP policies per partition.
- Define common applications and application groups with per partition processing and accounting.

ISA-AA partitions support accounting and customized reporting for every AA subscriber associated with a partition. You can perform the following operations:

- Define different types of reporting and accounting policies for different partitions in a single AA group.
- Display AA group level protocol statistics with partition visibility (for example, you can view protocol counts that are reported for each partition of the group).

When you create or delete an ISA-AA partition, a default AA accounting policy is automatically created in or deleted from the ISA-AA partition. See Procedure 18-2 for information about how to create and configure ISA-AA groups and partitions.

AA protocol signatures

The 5620 SAM generates a set of signatures that identify AA protocols. The signature set includes:

- protocol support summary—list of protocols that can be identified with the load using a combination of pattern and behavioral techniques. The protocols are used to generate statistics by protocol and as input in combination with other information to identify applications.
- pattern signatures—set of pattern-match signatures used in analysis
- behavior signatures—set of diagnostic techniques used in analysis

Dynamic upgrades of protocol signatures are implemented by using an admin application-assurance upgrade command and then performing ISA-AA activity switches. Protocol signatures are updated as part of an ISSU that only updates ISA-AA software. Signature upgrades without an NE upgrade can be performed within a major release independent of system ISSU limits.

Because protocol signatures are intended to be the most basic block of application identification, other AA components, such as application filters, are provided to further customize protocol signatures. Customization reduces the need for a new protocol signature load when a new application may need to be identified.

Each protocol can be referenced in the definition of one or more applications by the application filter definition. The assignment of each supported protocol to an application filter or application is optional, allowing for the addition of new signature protocols without the need to update the application filter and applications.

Protocol shutdown

The 5620 SAM supports signature upgrades without automatically affecting policy behavior. All post-R1 new signatures are disabled, by default, during an upgrade to ensure that policies or services are not affected.

The protocols that are included in R1 of a release are designated as parent signatures and cannot be disabled. Within a major release, all protocols introduced after R1 of a release as part of an isa-aa.tim ISSU are, by default, shut down. When shut down, protocols introduced after R1 do not change AA behavior. For example, traffic maps to the parent protocol on which the new signature is based. Enabling or disabling a new protocol takes affect for new flows only. The protocols must be enabled on a per-protocol basis to take effect. Perform Procedure 77-18 to enable AA protocols.

AA group policies

An AA group policy includes the following components:

- application filters
- applications
- application groups
- application profiles
- application service options
- application QoS policies
- custom protocols

Application filters

Application filters are provided as an indirect action between protocols and applications to allow the addition of variable parameters (for example, port numbers and IP addresses) to an application definition. Application filters are numbered rule entries that define the use of protocol signatures and other application criteria. Multiple application filter entries can be used to define an application, but each application filter entry maps to one application.

A traffic flow may have multiple rules. The rule with the lowest entry number that matches is applied. A traffic flow can only be assigned to one application.

Applications

Applications define and assign a description to the application names that are supported by the application filter entries. Each application is associated with one of the application groups. Applications are used by AA to identify the type of IP traffic in the subscriber traffic.

The application name is a key match criterion within the AQP rules that are applied to the IP traffic of a subscriber. The application name is also the unique identifier of the application object for northbound reporting systems such as the 5670 RAM. Changing an application name results in the loss of the previous application and the creation of a new application.

One predefined application (“unknown”) is provided by AA. The unknown application cannot be modified. All other applications must be configured. An application must be configured before the associated application filter is defined.

Network operators can:

- change the application group that an application is associated with
- view which application filters are defining the application

Application groups

An application group is a container for multiple applications. A set of default application groups is provided by AA. At least one default application group (“unknown”) must be associated with each NE. The default application groups cannot be modified.

Multiple applications can be assigned to an application group. An application can only belong to one group. Applications that are not assigned to an application group are automatically placed in the “unknown” application group.

Application profiles

Application profiles enable AA service for traffic to and from an ESM subscriber, SAP, or spoke SDP. Each application profile is unique and defines the AA service that the AA subscriber receives. The type of traffic is configured in the system-wide configuration of QoS forwarding classes to be diverted to the ISA-AA MDA for subscribers with AA enabled. The forwarding class is used for any subscriber traffic that a service provider needs to inspect using AA.

An ESM subscriber can be assigned to an application profile that affects every host of the subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned that affects the traffic originating from or destined over the SAP or spoke SDP.

For subscribers with application profiles that enable AA, traffic is diverted to the active ISA-AA MDA using ingress QoS policy filters. The filters identify forwarding and sub-forwarding classes that can be diverted for AA. The system identifies and diverts only traffic for any subscriber who is treated by the ISA-AA MDA, according to the application profile of the subscriber. Diversion to the ISA-AA MDA depends on the ISA-AA MDA status. If a subscriber is not configured to divert traffic to the ISA-AA MDA, normal ingress forwarding occurs.

The characteristics of application profiles are:

- By default, subscribers are not assigned to an application profile and traffic is not diverted for AA analysis.
- One or more application profiles can be configured.
- Application profiles are customer-defined and created using the configured application service options characteristics.
- Application profiles allow ASO characteristics to be associated with AA subscribers.
- Local instances of the application profile are configured to bind to specific objects of an NE (for example, L2 access interface, SAP, local subscriber explicit map entry, and so on).
- Application profiles can only be assigned when ISA-AA cards are assigned to an ISA-AA group
- Global application profiles must be manually distributed to the NEs.
- Application profiles can be assigned a capacity cost for subscriber load balancing among ISAs within the AA group.

ASOs

Application service options (ASOs) are used to define service provider and customer network functionality that is common among sets of subscribers. ASOs prevent subscribers from requiring each subscriber-specific entry in the application QoS policies for standard network services.

In a typical application, ASOs define the HSI service parameters.

- ASOs are optional; AA can check the subscriber IP traffic without the use of application service options.
- ASOs can be configured for each AA group policy.
- ASOs are a series of user-defined application characteristics.
- ASO characteristics are used to create application profiles and provide information to user-defined AQP rules.
- The set of ASOs represent network-wide menus of service capabilities that are available to subscribers.

Some examples of ASOs are:

- entry for each application group to be managed; for example, VoIP, P2P, and HTTP
- multiple entries (typically less than 20) where specific applications in an application group can be individually managed as service parameters; for example, HTTP content from a specific content provider or streaming video from network television or games
- HSI tiers (for example, Gold, Silver, and Bronze) that specify bandwidth levels
- bandwidth parameters for each service option

ASO characteristics are used:

- as input to application profiles
- by application QoS policies to influence how specific traffic is checked and how policies are applied

ASOs are defined and assigned to one or more values to define service offerings to customers.

You can configure ASO characteristics for an AA subscriber using an AA subscriber policy override. An AA subscriber policy override can be configured for a SAP or spoke SDP binding, but not for an ESM subscriber. The AA subscriber must have an application profile assigned, or the subscriber policy override is rejected.

You can retrieve on demand the ASO values that are assigned to an AA subscriber from the Edit form of the SAP or spoke SDP binding AA subscriber.

AQPs

Application Qos Policies, or AQPs, are lists of rules that define the match criteria and action to be performed on all traffic flows. The AQP rules use as the match criteria the application groups, applications, and so on. The output of the AQP rules defines the policy actions to perform.

AQP rules consist of match and action criteria:

- Match—Refers to the criteria used to identify a flow in order to apply actions such as dropping, forwarding, mirroring, and policing of bandwidth and flow. Matches cannot be made against protocols. Match criteria can be a combination of the following:
  - applications or application groups
  - ASO characteristics
  - flow direction
  - AA subscribers
  - flow source or destination IP address and/or port
- Action—Defines AA actions to be applied to traffic. For example, you can apply a set of actions such as bandwidth policing, packet discards, QoS remarking, and flow count, and/or rate limiting to a flow.

Custom protocols

Custom protocols are supported using configurable strings (up to 16 hexadecimal octets) for pattern-matched application identification in the payload of TCP- or UDP-based applications. The match is specified for the client-to-server, server-to-client, or any direction for TCP based applications, and in the “any” direction for UDP-based applications.

You can configure a custom protocol description, custom protocol ID and shutdown. When a custom protocol’s administrative status is disabled, traffic is identified as if the protocol is not configured.

Custom protocols and Alcatel-Lucent-provided protocols are distinct in that the span of a custom protocol is limited to the group or partition associated with an AA policy, while Alcatel-Lucent-provided protocols span all groups and partitions. Custom protocols are used in the application definition without limitations. All application filter entries, except strings, are supported. Custom protocol statistics collection on an ISA-AA partition group or special study subscriber is supported.

Reporting attributes

Reporting attributes are metadata parameters for reporting data to the 5670 RAM. The parameters are used to enhance the granularity of data analysis and are not deployable to devices. Reporting attributes can be found and configured individually in the 5670 RAM Parameters tab in the properties forms of the following objects:

- residential subscriber instances
- services
- SAPs
- customers
- applications
- application groups

Reporting attributes for service class and bandwidth are found on AA reporting objects that you can configure in the Reporting subtab of the 5670 RAM Parameters tab in the properties forms of the following objects:

- spoke SDP bindings
- L3 access interfaces
- VPN-type transit prefix subscribers

Note 1 — You must associate an application profile with the following objects before you can configure AA reporting objects.

Note 2 — You cannot create more than one AA reporting object for a service or subscriber object.

See the configuration procedures for the above objects for more information about configuring reporting attributes.

Usage-based billing

The 5620 SAM supports application-specific reporting to the 5670 RAM based on configurable charging groups. The 5620 SAM automatically assigns a set of eight default charging groups to each application profile. You can configure charging groups with specific usage quotas and thresholds, and assign the charging groups to applications and application groups. Applications and application groups are assigned to the first charging group by default, and can only be assigned to one charging group. You cannot create additional charging groups.

Policy Sync Group

Policy sync groups allow AA group policy components to be centrally defined and used across multiple ISA-AA groups and partitions. Policy sync groups define common AA group policy components by specifying a group policy as the master policy. The applications, application groups, custom protocols, and application filters of the master AA group are available to other AA groups that are members of the same policy sync group.

Use the Policy Sync Group menu option to designate an AA group policy as the master policy and add one or more AA group policies to Policy Sync Group members. You can overwrite or add the contents of the master policy to one or more of its members.

AA policers

AA policers can be bandwidth or flow limiting, and can have one of the following scopes:

- system scope—limits all traffic entering the ISA-AA MDA
- subscriber scope—limits apply to the traffic of a subscriber

After a policer is referred to by an AQP for one traffic direction, the same policer cannot be referred to in the other direction. AQP rules with policer actions must specify a traffic direction other than “both”.

AA accounting policies

The AA accounting statistics provide information required to understand the application use in a network. You can configure AA accounting to collect and report statistics when at least one ISA-AA MDA is active. The AA accounting statistics provide information about application use on a SAP or spoke SDP, or by a subscriber during a collection interval. The collected information can be viewed in graphical or tabular form using the 5620 SAM GUI, or sent to a module such as the 5670 RAM for reporting and trend analysis.

AA accounting collects statistics on traffic flows. The 5620 SAM can collect the following AA statistics types:

- AA application
- AA application group
- AA protocol
- AA subscriber protocol (special-study)

- AA subscriber application (special-study)
- AA subscriber custom record

AA uses the existing 5620 SAM and NE accounting statistics and logging capabilities to collect statistics. See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics. See Procedure 77-5 for information about configuring an AA accounting policy.

The 5620 SAM can be configured to generate statistics for each protocol and application for a specific subscriber. You can enable AA statistics collection on a specific NE for a subset of subscribers for detailed traffic monitoring. An NE can have one policy for each AA statistics type that is enabled.

The AA subscriber protocol and AA subscriber application statistics are special study statistics for detailed accounting statistics collection on a limited number of subscribers, SAPs , or spoke SDPs on an NE. The number of subscribers, SAPs, or spoke SDPs is limited to constrain the volume of generated statistics.

Special study statistics are enabled by adding subscribers, SAPs, or spoke SDPs to a list in an ISA-AA group on an NE for AA debugging purposes. When a subscriber is on a special study list, the ISA-AA creates one statistics record for each application and application group that is associated with the subscriber. When a SAP or spoke SDP is on a special-study list, the ISA-AA creates one statistics record for each application, application group, and protocol flow on the SAP or spoke SDP. See Procedure 18-2 for information about configuring special study objects in an ISA-AA group.

An AA custom record subscriber accounting policy applies to all subscribers, SAPs and spoke SDPs in an ISA-AA group for a specified set of AA protocols, applications, and application groups. The policy enables statistics collection on only the specified objects, which limits the volume of collected data and the statistics collection processing load. For example, a 5620 SAM operator may require statistics for only three application groups and 10 applications. You can view and configure the AA statistics objects from the AA Subscriber Stats Objects tab on the properties form of an ISA-AA group.

AA flow watermark policies

AA supports the configuration of high and low thresholds (watermarks) for logs and traps when there is a high consumption of the flow table. The flow table has a limited size and the thresholds are established to alert users that the flow table is approaching maximum capacity. When the high threshold is reached, an alarm is generated. The alarm is cleared when the flow table capacity has dropped below the specified low threshold.

AA transit IP and transit prefix policies

AA transit IP and transit prefix policies define how AA transit subscribers are created by an NE. Transit IP policies can be configured to discover dynamic transit subscribers via DHCP or RADIUS, and can also be configured with a list of static transit subscribers. Transit prefix policies allow you to specify transit subscribers by using network or subscriber IP ranges.

AA transit subscribers can persist in the 5620 SAM database. Transit subscriber aggregators allow you to aggregate multiple database persisted transit subscriber instances for VPN sites.

Application performance reporting

Application performance reporting adds a layer of route configuration to the handling of AA TCP performance, RTP/UDP performance, and flow-based volume reporting to the 5670 RAM. You can enable application performance reporting on service objects, and the configure default DCP groups with address rules to apply a DCP subnet group to an entire network, an IP address range, or a single IP address for Internet or intranet traffic.

You can also create custom DCP subnet groups and bind them to individual L3 access interfaces and spoke SDP bindings. The 5670 RAM ignores application performance reporting configuration and objects on services that do not, or cannot, have an associated application profile.

AA HTTP error redirect policies

AA HTTP error redirect policies allow you to specify templates for local NE termination of HTTP errors and web browser redirection to customized error pages according to HTTP error codes.

77.2 Workflow to configure application assurance

1 Configure ISA-AA groups on NEs. See Procedure 18-2.

2 Configure AA group policies by performing Procedure 77-1. As required, configure the following components:

i ASOs and ASO overrides

ii application profiles

iii application groups

iv applications

v application filters

vi custom protocols

3 Configure AA policers. See Procedure 77-2.

4 Configure AQPs for AA group policies. See Procedure 77-3.

5 Create a policy sync group. See Procedure 77-4.

6 Create an AA accounting policy to specify when statistics are to be collected on the ISA-AA MDA. See Procedure 77-5.

7 Configure an AA flow watermark policy. See Procedure 77-6.

8 Configure AA transit IP policies and transit prefix policies as required.

i Configure AA transit IP policies. See Procedure 77-7.

ii Configure AA transit prefix policies. See Procedure 77-8.

iii Configure database persisted transit subscriber aggregators. See Procedure 77-9.

iv Associate database persisted transit subscribers with aggregators. See Procedure 77-10.

v Configure reporting attributes for AA reporting on a database persisted transit subscriber. See Procedure 77-11.

vi As required, view the database persisted transit subscriber information. See Procedure 77-12.

9 Configure usage-based billing as required:

i Enable usage-based billing at the application profile level. See Procedure 77-13.

ii Associate applications and application groups with charging groups. See Procedure 77-14.

10 Configure application performance reporting on a service. See Procedure 77-15.

11 Create a custom DCP subnet group for application performance reporting on a service and related objects. See Procedure 77-16.

12 Configure AA HTTP error redirect policies. See Procedure 77-17.

13 Configure AA protocol signatures and enable inactive protocols, as required. See Procedure 77-18.

14 As required, view AA results:

a view AA summary information for subscribers, transit subscribers, SAPs, and spoke SDPs on ISA-AA MDAs; see Procedure 77-19 for more information

b view the AA special study statistics data for subscribers, transit subscribers, SAPs, or spoke SDPs on an ISA-AA MDA; see Procedure 77-20 for more information

c view application filter hit counts on local definitions of AA group policies; see Procedure 77-21 for more information

d view application filter hit counts on local definitions of AA group policies; see Procedure 77-22 for more information

15 As required, delete AA objects or records:

a delete an AA application, application group, or custom protoco; see Procedure 77-23 for more information

b remove the record of an inactive AA transit subscriber from the 5620 SAM database; see Procedure 77-24 for more information

77.3 Application assurance procedures

Use the following procedures to configure AA policies and parameters in the 5620 SAM.

Procedure 77-1 To configure an AA group policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

> **Note —** The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select the policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Configure the Description parameter.

5 Perform the following steps to create an application group.

- **i** Click on the Application Groups tab button.

- **ii** Click on the Create button. The Application Group (Create) form opens.

> **Note —** You can also create an application group from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Application Groups and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Application Groups.

- **iii** Configure the parameters:
  - Displayed Name
  - Description

- **iv** Click on the 5670 RAM Parameters tab button.

- **v** Configure the parameters:
  - Charging Group
  - Traffic Type

- **vi** Click on the OK button. A dialog box appears.

- **vii** Click on the OK button. The AA Group Policy (Edit) form reappears.

6 Repeat step 5 to create additional application groups, as required.

7 Perform the following steps to create an application.

i Click on the Applications tab button.

ii Click on the Create button. The Application (Create) form opens.

Note — You can also create an application from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Applications and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Applications.

iii Configure the parameters:

- Displayed Name
- Description

iv Click on the Application Groups tab button.

v Click on the Select button in the Application Group panel to choose an application group. The Select Application Group search form opens.

vi Select an application group in the list and click on the OK button. The Select Application Group form closes and the application group information appears on the Application (Create) form.

vii Click on the 5670 RAM Parameters tab button.

Note — The 5670 RAM can perform an application performance index analysis on an AA application. An application performance index configuration is not distributed to an NE as part of a policy distribution.

The 5670 RAM provides a comparative analysis of TCP and UDP application usage. For each application, you can specify whether the application is TCP or UDP. TCP or UDP data is not distributed to an NE as part of a policy distribution.

viii Configure the parameters:

- Application Flag
- Traffic Type
- Round Trip Time Tolerated (milliseconds)
- Mean Total Delay Tolerated (milliseconds)
- Total Delay Standard Deviation Tolerated (milliseconds)
- Packet Loss Tolerated (%)
- Charging Group
- Threshold Administrative State
- Frustrated (milliseconds)
- Frustrated (milliseconds)
- Frustrated (milliseconds)
- Frustrated (%)

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The AA Group Policy (Edit) form reappears.

8 Repeat step 7 to create additional applications, as required.

9 Perform the following steps to create an application filter.

i Click on the Application Filters tab button.

ii Click on the Create button. The Application Filter (Create) form opens.

Note — You can also create an application filter from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Application Filters and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Application Filters.

iii Configure the parameters:

- Entry ID
- Description
- Administrative State

iv Click on the General Properties tab button.

v Configure the parameters:

- Flow Set-up Direction
- IP Protocol Operator
- IP Protocol Number
- Protocol Operator
- Protocol Type
- Server Address Operator
- Server Address
- Server Address Mask
- Server Port Operator
- Server Port Value Type
- Server Port/Low Value
- Server Port High Value
- Server Port First Packet Policy

vi Click on the Select button in the Protocol panel to choose a protocol. The Select Protocol form opens.

vii Select a protocol in the list and click on the OK button. The Select Protocol form closes and the protocol information appears on the Application Filter (Create) form.

viii Click on the Select button in the Protocol panel to choose a custom protocol name. The Select Custom Protocol form opens.

ix Select a custom protocol in the list and click on the OK button. The Select Custom Protocol form closes and the protocol information appears on the Application Filter (Create) form.

x Click on the Application tab button.

xi Click on the Select button in the Application panel to choose an application. The Select Application search form opens.

xii Select an application in the list and click on the OK button. The Select Application form closes and the application information appears on the Application Filter (Create) form.

xiii Click on the Application Filter Expressions tab button.

xiv Click on the Create button. The Application Filter Expression (Create) form opens.

xv Configure the parameters:

- Index
- Type
- Operator
- String

xvi Click on the OK button. The Application Filter Expression (Create) form closes and the expression information appears on the Application Filter (Create) form.

xvii Repeat step 9 xiv to xvi to create an additional application filter expression, if required. The maximum number of application filter expressions that can be created is 3.

xviii Click on the OK button. A dialog box appears.

xix Click on the OK button. The Application Filter (Create) form reappears.

10 Repeat step 9 to create an additional application filter, if required.

11 Perform the following steps to create an application service option.

i Click on the Application Service Options tab button.

ii Click on the Create button. The Application Service Option (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- ASO Characteristic Default Value

iv Click on the Application Service Option Value Entries tab button.

v Click on the Create button. The Application Service Option Value Entry (Create) form opens.

vi Configure the ASO Characteristic Value parameter.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Application Service Option Value Entry (Create) form closes and the entry information appears on the Application Service Option (Create) form.

ix Repeat steps 11 iv to viii to create an additional application service option value entry.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The AA Group Policy form reappears.

12 Repeat step 11 to create an additional application service option.

13 Perform the following steps to create an application profile.

i Click on the Application Profiles tab button.

ii Click on the Create button. The Application Profile (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- Description
- Divert
- Capacity Cost

iv Click on the Characteristics tab button.

v Click on the Create button. The Application Profile Characteristic (Create) form opens.

vi Click on the Select button beside the ASO Characteristic parameter. The Select Application Service Option search form opens.

vii Select an application service option in the list and click on the OK button. The Select Application Service Option form closes and the application service option information appears on the Application Profile Characteristic form.

viii Click on the Select button beside the ASO Characteristic Value parameter. The Select Application Service Option Characteristic Value search form opens.

ix Select an ASO characteristic value in the list and click on the OK button. The Select Application Service Option Characteristic Value form closes and the ASO characteristic value information appears in the Application Profile Characteristic form.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Application Profile Characteristic (Create) form closes and the entry information appears on the Application Profile (Create) form.

xii Repeat steps 13 v to xi to create an additional application profile characteristic, if required.

xiii Click on the OK button. A dialog box appears.

xiv Click on the OK button. The AA Group Policy form reappears.

14 Repeat step 13 to create an additional application profile, if required.

15 Create custom protocols.

i Click on the Custom Protocols tab button.

ii Click on the Create button. The Custom Protocol (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Description
- IP Protocol Number
- Administrative State

iv Click on the Custom Protocol Expressions tab button.

v Click on the Create button. The Custom Protocol Expressions (Create) form opens.

vi Configure the parameters:

- Index
- Custom Protocol Expression Offset
- Custom Protocol Expression Direction
- Operator
- String

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Custom Protocol Expression (Create) form closes and the entry information appears on the Custom Protocol (Create) form.

ix Click on the OK button. The AA Group Policy form reappears.

16 Modify a local instance of an AA group policy, as required.

i Click on the Local Definitions tab. The AA policies for each managed NE are listed.

ii Select an AA policy in the list and click on the Properties button to modify the local instance of the policy.

iii Perform steps 4 to 14. Go to step 17.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The AA Group Policy form closes and the Application Assurance Policies form reappears.

19 Close the Application Assurance Policies form.

Procedure 77-2 To create an AA policer policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Policer (Application Assurance) from the object drop-down list

3 Click on the Create button and choose Create AA Policer. The AA Policer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ISA-AA Group ID
- Displayed Name
- Type
- Granularity
- Description

Note — The distribution of an AA policer fails if the ISA-AA group ID it refers to does not exist on the NE.

5 Perform one of the following:

a If the Type parameter was set to Dual Bucket Bandwidth, go to step 7.

b If the Type parameter was set to Flow Count Limit, configure the Flow Count (flows) parameter.

c If the Type parameter was set to Flow Rate Limit, go to step 9.

d If the Type parameter was set to Single Bucket Bandwidth, go to step 11.

6 Go to step 12.

7 Configure the parameters:

- MBS (KB)
- CBS (KB)
- PIR (Kbps)
- CIR (Kbps)
- PIR
- CIR

8 Go to step 12.

9 Configure the parameters:

- MBS (flows)
- PIR (Kbps)
- PIR

10 Go to step 12.

11 Configure the parameters:

- Action
- MBS (KB)
- PIR (Kbps)
- PIR

12 Click on the OK button to close the AA Policer (Create) window.

13 Close the Application Assurance Policies form.

Procedure 77-3 To create an AQP

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select the policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Click on the Application QoS Entries tab button.

5 Click on the Create button. The Application QoS Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Administrative State

7 Click on the Match Criteria tab button.

8 Configure the parameters:

- Traffic Direction
- Application Operator

9 Click on the select button beside the Displayed Name parameter in the Application panel. The Select Application Name - Application QoS Policy list form opens.

10 Select an application from the list and click on the OK button. The Select Application Name - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

11 Configure the Application Group Operator parameter.

12 Click on the select button beside the Displayed Name parameter in the Application panel. The Select Application Group Name - Application QoS Policy list form opens.

13 Select an application group from the list and click on the OK button. The Select Application Group Name - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

14 Configure the parameters in the DSCP panel:

- DSCP Operator
- DSCP

15 Click on the AA Subscriber tab button.

16 Configure the SubscriberType parameter.

Note 1 — The SAP and Spoke SDP Binding options are valid for the SubscriberType parameter only when you create a local AQP entry.

Note 2 — If the SubscriberType parameter is set to None, the values of all parameters on the AA Subscriber tab are reset.

17 Perform one of the following:

a If the SubscriberType parameter is set to ESM, go to step 18.

b If the SubscriberType parameter is set to SAP, go to step 20.

c If the SubscriberType parameter is set to Spoke SDP Binding, go to step 21.

d If the SubscriberType parameter is set to Transit, go to step 22.

e If the SubscriberType parameter is set to None, go to step 23.

18 Configure the parameters:

- Subscriber Operator
- ESM Subscriber

19 Go to step 23.

20 Configure the parameters:

- Subscriber Operator
- SAP Subscriber

21 Configure the parameters:

- Subscriber Operator
- Spoke Subscriber

22 Configure the parameters:

- Subscriber Operator
- Transit Subscriber

23 Click on the Source and Destination tab button.

24 Configure the parameters in the Source Address panel:

- Address Operator
- Address
- Address Length

25 Configure the parameters in the Source Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

26 Configure the parameters in the Destination Address panel:

- Address Operator
- Address
- Address Length

27 Configure the parameters in the Destination Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

28 Click on the Characteristics tab button.

29 Click on the Create button.

30 Configure the parameters:

- ASO Characteristic
- ASO Characteristic Operator
- Capacity Cost

31 Click on the Action tab.

32 Configure the Drop parameter.

33 Click on the Select button beside the Displayed Name parameter in the Bandwidth Limit Policer panel. The Select Bandwidth Limit Policer - Application QoS Policy list form opens.

34 Select a bandwidth limit policer from the list and click on the OK button. The Select Bandwidth Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

35 Click on the Select button beside the Displayed Name parameter in the Flow Rate Limit Policer panel. The Select Flow Rate Limit Policer - Application QoS Policy list form opens.

36 Select a flow rate limit policer from the list and click on the OK button. The Select Flow Rate Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

37 Click on the Select button beside the Displayed Name parameter in the Flow Count Limit Policer panel. The Select Flow Count Limit Policer - Application QoS Policy list form opens.

38 Select a flow count limit policer from the list and click on the OK button. The Select Flow Count Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

39 Click on the Select button beside the Displayed Name parameter in the HTTP Error Redirect panel. The Select HTTP Error Redirect - Application QoS Policy list form opens.

40 Select an HTTP error redirect policy from the list and click on the OK button. The Select HTTP Error Redirect - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

41 Click on the Select button beside the Service ID parameter in the Mirror Source panel. The Select Service ID - Application QoS Policy list form opens.

42 Select a mirror service from the list and click on the OK button. The Select Service ID - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Service ID information.

Note — The Service ID parameter can only be configured when creating a local AQP entry.

43 Configure the parameters:

- Mirror Source All Inclusive
- Forwarding Class
- Priority
- Remark DSCP In Profile
- Remark DSCP Out Profile

44 Click on the OK button to close the Application QoS Policy (create) form.

45 Click on the OK button to close the AA Group Policy (Edit) form.

46 Close the Application Assurance Policies form.

Procedure 77-4 To create a policy sync group

1 Choose Policies→Policy Sync Group from the 5620 SAM main menu. The Policy Sync Groups form opens.

2 Perform the following steps to create a Policy Sync Group.

i Click on the Create→Create Policy Sync Group. The Policy Sync Group (Create) form opens.

ii Configure the parameters:

- Auto-Assign ID
- Description
- Displayed Name

iii Click on the Select button in the Master Policy panel to choose a master policy. The Select Master Policy - Policy Sync Group form opens.

iv Choose a master policy in the list and click on the OK button. The Select Master Policy - Policy Sync Group closes and the Policy Sync Group (Create) form reappears.

v Click on the OK button. The Policy Sync Group Manager form reappears.

3 Add a member to a master AA group policy.

i From the Policy Sync Group Manager form, choose a Policy Sync Group from the list and click on the Properties button. The Policy Sync Group (Edit) form opens with the General tab displayed.

ii Click on the Members tab.

iii Click on the Create button. The Select AA Group Policy - Policy Sync Group form opens.

iv Choose one or more AA group policies in the list and click on the OK button. A dialog box appears.

v Choose one of the options and click on the OK button. The Select AA Group Policy - Policy Sync Group form closes and the member is displayed on the Policy Sync Group (Edit) form.

Note 1 — The Sync Members button performs the same function as the “Listed master policy classes will overwrite member classes” option. The Add to Members button performs the same function as the “Listed master policy classes will be added to member classes” option.

Note 2 — The Sync Members, Add to Members, and Update Master actions performed on an AA group policy only affect the classes listed under the Included Classes tab button.

4 Audit and compare a master AA group policy and its members for the classes listed under the Included Classes tab.

Note 1 — The Audit button displays the differences between a master AA group policy and its members.

Note 2 — The Compare button compares two selected policies between master-member, or member-member.

Note 3 — The Update Master button adds the contents of a selected AA group policy to the included classes of a master policy.

i Click on the Audit button. A dialog box appears.

ii Click on the Yes button. An Audit dialog box appears.

iii Click on the OK button.

iv View the alarm window to display the alarms raised against the member policy, if required.

5 Compare and view detailed differences between two policies.

i Hold down the Shift key to choose two policies in the list and click on the Compare button. The Compare - AA Group Policy form opens.

ii Click on the Compare button to view the differences between Policy A and Policy B.

Note 1 — You can use the Swap button to switch Policy A and Policy B.

Note 2 — You can use the Difference drop-down list to choose a category that you need to filter on.

iii Choose a result and and click on the Properties button. The Difference - AA Group Policy (*class type*) form opens.

iv View the differences between the two policies.

Note — After a Sync Member or Add to Member action, the member policy mode changes to Draft. When the policy is in Draft mode, you must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 46 for more information.

Procedure 77-5 To configure an AA accounting policy

See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Accounting Policy (Application Assurance) from the object drop-down list.

3 Perform one of the following:

a To create an AA accounting policy, click on the Create button and choose Create AA Accounting Policy from the object drop-down list. The AA Accounting Policy (Create) form opens.

b To modify an AA accounting policy:

i Click on the Search button. The AA accounting policies are displayed.

ii Select an AA accounting policy in the list and click on the Properties button. The AA Accounting Policy (Edit) form opens.

4 Configure the parameters:

- Group ID
- Partition ID
- Description

5 Click on the Apply button. The form displays additional tabs.

6 Click on the Accounting Policies tab button. A list of accounting policies is displayed.

7 Configure each accounting policy in the list, if required.

i Select the accounting policy and click on the Properties button. The AA Accounting Configuration form is displayed.

ii Configure the parameters:

- Description
- Collect Accounting Statistics

iii Configure the following policy-specific parameters, if required:

- Administrative State
- Collect Aggregate Statistics
- Collect Maximum Throughput Statistics

iv Click on the Select button to choose an accounting policy. The Select Accounting Policy form opens.

v Select an accounting policy in the list and click on the OK button. The Select Accounting Policy form closes and the accounting policy information appears on the AA Accounting Configuration form.

vi Click on the OK button. The AA Accounting Configuration (Edit) form closes.

8 Click on the Apply button. A dialog box appears.

9 Click on the Yes button.

10 Click on the General tab button.

11 Click on the Switch Mode button. A dialog box appears.

12 Click on the Yes button.

13 Click on the Distribute button to manually distribute the policy to one or more NEs. The Distribute - AA Accounting form opens.

14 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

15 Click on the Distribute button. The policy is distributed to the NEs.

16 Modify a local instance of the AA accounting policy, if required.

i Click on the Local Definitions tab button. The AA accounting policies for each managed NE are listed.

ii Select an AA accounting policy in the list and click on the Properties button to modify the local instance of the policy. The AA Accounting Configuration (Edit) form opens.

iii Click on the Switch Mode button.

iv Perform steps 4 to 12.

17 Click on the OK button. The AA Accounting Configuration (Edit) form closes and the Application Assurance Policies form reappears.

18 Close the Application Assurance Policies form.

Procedure 77-6 To configure an AA flow watermark policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Flow Watermark (Application Assurance) from the object drop-down list.

3 Specify a filter to create a filtered list of flow watermark configurations, and click on the Search button. A list of flow watermark configurations is displayed.

4 Select an entry in the list and click on the Properties button. The AA Flow Watermark (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Flow Full High Watermark
- Flow Full Low Watermark
- Flow Setup High Watermark
- Flow Setup Low Watermark
- Packet Rate High Watermark
- Packet Rate Low Watermark
- Bit Rate High Watermark
- Bit Rate Low Watermark

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button.

8 Click on the General tab button.

9 Click on the Switch Mode button. A dialog box appears.

10 Click on the Yes button.

11 Click on the Distribute button to manually distribute the policy to one or more NEs. The Distribute - AA Flow Watermark form opens.

12 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

13 Click on the Distribute button. The policy is distributed to the NEs.

14 Modify a local instance of the AA flow watermark configuration, if required.

i Click on the Apply button.

ii Click on the Local Definitions tab. The AA flow watermark configurations for each managed NE are listed.

iii Select a managed NE in the list and click on the Properties button to modify the local instance of the flow configuration.

iv Perform step 5.

v Click on the OK button. The Application Assurance Flow Configuration form closes.

15 Click on the OK button. The Application Assurance Flow Configuration form closes and the Application Assurance Policies form reappears.

16 Close the Application Assurance Policies form.

Procedure 77-7 To configure an AA transit IP policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

a Create an AA transit IP policy:

i Click on the Create button and choose AA Transit IP Policy from the object drop-down list. The AA Transit IP Policy (Create) form opens with General tab displayed.

ii Configure the parameters:

- Group ID
- Partition ID
- Auto-Assign ID
- Policy ID
- Description

b Modify an AA transit IP policy:

i Choose AA Transit IP Policy (Application Assurance) from the object drop-down list.

ii Click on the Search button to display a list of AA transit IP policies.

iii Select an AA transit policy in the list and click on the Properties button. The AA Transit IP Policy (Edit) form opens.

3 Click on the Select button in the Default Application Profile panel to choose an application profile. The Select Default Application Profile - AA Transit IP Policy form opens.

4 Choose an application profile from the list and click on the OK button.

Note — Only application profiles with the same Group ID and Partition ID values as the AA transit IP policy can be selected.

5 Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy. The Select Subscriber Identification Policy form opens.

6 Choose a subscriber identification policy from the list and click on the OK button.

7 Configure the parameters:

- DHCP
- RADIUS

Note — The DHCP and RADIUS parameters cannot be set to Enabled at the same time.

8 If the RADIUS parameter is set to Enabled, click on the Select button in the Subscriber Authentication Policy panel. The Select Subscriber Authentication Policy form opens.

9 Choose a subscriber authentication policy from the list and click on the OK button.

10 Add static subscribers to the AA transit IP policy:

i Click on the Subscribers tab button.

ii Click on the Create button. The Transit Subscriber (Create) form opens with the General tab displayed.

iii Configure the Displayed Name parameter.

iv Click on the Select button in the Application Profile panel. The Select Application Profile form opens.

v Choose an application profile from the list and click on the OK button.

vi Click on the IP Addresses tab button.

vii Click on the Create button. The Transit IP Address (Create) form opens.

viii Configure the Address parameter.

ix Click on the OK button.

x Return to step vii and add more addresses, as required.

xi Click on the OK button. The Transit Subscriber (Create) form closes.

11 Repeat step 10 to add more static subscribers to the AA transit IP policy, as required.

12 Click on the Apply button to save the AA transit IP policy. If you are modifying a transit IP policy, a dialog box appears.

13 Click on the Yes button, if required.

14 Click on the General tab button.

15 Click on the Switch Mode button. A dialog box appears.

16 Click on the Yes button.

17 Click on the More Actions button and choose Distribute to manually distribute the policy to one or more NEs. The Distribute - AA Transit IP Policy form opens.

18 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

19 Click on the Distribute button. The policy is distributed to the NEs.

20 Modify a local instance of the AA transit IP policy, if required.

- **i** Click on the Local Definitions tab button. The AA transit IP policies for each managed NE are listed.
- **ii** Choose an AA transit IP policy from the list and click on the Properties button to modify the local instance of the policy. The AA Transit IP Policy (Edit) form opens.
- **iii** Click on the Switch Mode button.
- **iv** Perform steps 3 to 16.

21 Click on the OK button. The AA Transit IP Policy (Edit) form closes and the Application Assurance Policies form reappears.

22 Close the Application Assurance Policies form.

Procedure 77-8 To configure an AA transit prefix policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Perform one of the following:

- **a** Create an AA transit prefix policy:
  - **i** Click on the Create button and choose AA Transit Prefix Policy. The AA Transit Prefix Policy (Create) form opens with the General tab displayed.
  - **ii** Configure the parameters:
    - Group ID
    - Partition ID
    - Auto-Assign ID
    - Policy ID
    - Description

iii Click on the Apply button. The form changes to the AA Transit Prefix Policy (Edit) and refreshes with additional tabs.

iv Go to step 3.

b Configure an existing AA transit prefix policy:

i Choose AA Transit Prefix Policy (Application Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button to generate a list of AA transit prefix policies.

iii Select an AA transit prefix policy from the list and click on the Properties button. The AA Transit Prefix Policy (Edit) form opens with the General tab displayed.

iv Go to step 3.

3 Perform the following steps to configure subscribers:

i Click on the Subscribers tab button.

ii Click on the Create button. The Transit Prefix Subscriber (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Remote

iv Click on the Select button in the Application Profile panel. The Select Application Profile - Transit Prefix Subscriber form opens.

v Configure the filter criteria, if required, and click on the Search button to generate a list of application profiles.

vi Select an application profile from the list and click on the OK button. the Select Application Profile - Transit Prefix Subscriber form closes and the Transit Prefix Subscriber (Create) form refreshes with the selected application profile.

vii Click on the OK button.

viii Repeat steps ii to vii to create additional transit prefix subscribers, as required.

4 Perform the following steps to create transit prefix entries:

i Click on the Entries tab button.

ii Click on the Create button. The Transit Prefix Policy (Create) form opens.

iii Click on the Select button in the Subscriber panel. The Select Subscriber - Transit Prefix Entry form opens.

iv Configure the filter criteria, if required, and click on the Search button to generate a list of subscribers.

v Select a subscriber and click on the OK button.

vi Configure the parameters:

- Auto-Assign ID
- Match Subscriber Address
- Subscriber Address Prefix Length
- Network Address
- ID
- Subscriber Address
- Match Network Address
- Network Address Prefix Length

vii Click on the OK button.

viii Repeat steps ii to vii to create additional transit prefix entries, as required.

5 Click on the Apply button. If you are modifying an AA transit prefix policy, a dialog box appears.

6 Click on the Yes button. if required.

7 Click on the General tab button.

8 Click on the Switch Mode button. A dialog box appears.

9 Click on the Yes button.

10 Click on the Distribute button to manually distribute the policy to one or more NEs. The Distribute - AA Transit Prefix Policy form opens.

11 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

12 Click on the Distribute button. The policy is distributed to the NEs.

13 Modify a local instance of the AA transit prefix policy, if required.

i Click on the Local Definitions tab button. The AA transit prefix policies for each managed NE are listed.

ii Choose an AA transit prefix policy from the list and click on the Properties button to modify the local instance of the policy. The AA Transit Prefix Policy (Edit) form opens.

iii Click on the Switch Mode button.

iv Perform steps 3 to 9.

14 Click on the OK button. The AA Transit Prefix Policy (Edit) form closes and the Application Assurance Policies form reappears.

15 Close the Application Assurance Policies form.

Procedure 77-9 To configure a database persisted transit subscriber aggregator

1 Choose Manage→AA Transit Subscriber from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Perform one of the following:

a Create a database persisted transit subscriber aggregator:

i Click on the Create button and choose Transit Subscriber Aggregator. The Database Persisted Transit Subscriber Aggregator (Create) form opens with the General tab displayed.

ii Configure the Name parameter.

iii Click on the Apply button. The form refreshes as the Database Persisted Transit Subscriber Aggregator (Edit) form.

iv Go to step 3.

b Modify a database persisted transit subscriber aggregator:

i Choose Database Persisted Transit Subscriber Aggregator (Application Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button. A list of database persisted transit subscriber aggregators is displayed.

iii Select a database persisted transit subscriber aggregator from the list and click on the Properties button. The Database Persisted Transit Subscriber Aggregator (Edit) form opens with the General tab displayed.

iv Go to step 3.

3 Configure the parameters:

- Description
- Keyword List

4 Click on the Apply button. A dialog box appears.

5 Click on the Yes button.

6 Click on the Transit Subscribers tab button.

7 Configure the filter criteria, if required, and click on the Search button. A list of the database persisted transit subscribers that are associated with the database persisted transit subscriber aggregator is displayed.

8 Close the Database Persisted Transit Subscriber Aggregator (Edit) form.

9 Close the Manage AA Transit Subscribers form.

Procedure 77-10 To associate a database persisted transit subscriber with an aggregator

Note — You can only associate an aggregator object with database persisted transit subscribers that belong to ISA-AA groups that are configured with a Subscriber Scale of VPN.

1 Choose Manage→AA Transit Subscriber from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of database persisted transit subscribers is displayed.

4 Select a database persisted transit subscriber from the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 Click on the 5670 RAM Parameters tab button.

6 Click on the Select button. The Select Database Persisted Transit Subscriber Aggregator form opens.

7 Configure the filter for the Keywords List column and click on the Search button. A list of database persisted transit subscriber aggregators is displayed.

8 Select an aggregator from the list and click on the OK button.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button.

11 Repeat steps 3 to 10 to associate more database persisted transit subscribers with aggregators, as required.

12 Close the Manage AA Transit Subscribers form.

Procedure 77-11 To configure reporting attributes for AA reporting on a database persisted transit subscriber

Note — You can only perform this procedure for VPN-type transit subscribers.

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of database persisted transit subscribers is displayed.

4 Select a database persisted transit subscriber from the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 Click on the 5670 RAM Parameters tab button.

6 Click on the Reporting tab button.

7 Click on the Create button. The AA Reporting (Create) form opens.

8 Configure the parameters:

- Customer Name
- Subscriber Class
- Total Bandwidth Upstream (Kbps)
- Class of Service 1 Bandwidth Upstream (Kbps)
- Class of Service 2 Bandwidth Upstream (Kbps)
- Class of Service 3 Bandwidth Upstream (Kbps)
- Class of Service 4 Bandwidth Upstream (Kbps)
- Subscriber Name
- Subscriber Type
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)
- Downstream (Kbps)

9 Click on the OK button. The AA Reporting (Create) form closes and the reporting object is displayed in the list.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The Database Persisted Transit Subscriber (Edit) form closes.

12 Close the Manage AA Transit Subscribers form.

Procedure 77-12 To view database persisted transit subscriber information

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Choose Database Persisted Transit Subscriber (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of database persisted transit subscribers is displayed.

4 Select a database persisted transit subscriber from the list and click on the Properties button. The Database Persisted Transit Subscriber (Edit) form opens with the General tab displayed.

5 View the subscriber information, as required.

6 Close the Database Persisted Transit Subscriber (Edit) form.

7 Close the Manage AA Transit Subscribers form.

Procedure 77-13 To configure usage-based billing for an application profile

You must perform this procedure on an existing application profile. Perform Procedure 77-14 to assign applications and application groups to charging groups.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button to generate a list of AA group policies.

4 Select an AA group policy from the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

5 Click on the Application Profiles tab button.

6 Configure the filter criteria, if required, and click on the Search button to generate a list of application profiles.

7 Select an application profile from the list and click on the Properties button. The Application Profile (Edit) form opens with the General tab displayed.

8 Click on the 5670 RAM Parameters tab button.

9 Configure the Billing Reset Date parameter.

10 Click on the Charging Groups tab button. The form lists the default charging groups.

Note — The 5620 SAM creates charging groups on an application profile when the application profile is saved in the parent AA group policy.

11 Select a charging group from the list and click on the Properties button. The Charging Group (Edit) form opens.

12 Configure the parameters:

- Quota (GB)
- Threshold 1 (%)
- Threshold 2 (%)
- Threshold 3 (%)

13 Click on the OK button to save the changes and close the Charging Group (Edit) form.

14 Repeat steps 11 to 13 to configure additional charging groups, as required.

15 Click on the OK button to close the Application Profile (Edit) form.

16 Click on the OK button in the AA Group Policy (Edit) form. A dialog box appears.

17 Click on the Yes button to close the form.

Procedure 77-14 To associate an application or application group with a charging group

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button to generate a list of AA group policies.

4 Select an AA group policy from the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

5 To associate an application group with a charging group, perform the following steps:

   i Click on the Application Groups tab button.

   ii Select an application group from the list and click on the Properties button. The Application Group (Edit) form opens with the General tab displayed.

   iii Click on the 5670 RAM Parameters tab button.

   iv Configure the Charging Group parameter.

   v Click on the OK button to close the Application Group (Edit) form.

   vi Click on the Apply button in the AA Group Policy (Edit) form. A dialog box appears.

   vii Click on the Yes button to save the changes.

6 To associate an application with a charging group, perform the following steps:

   i Click on the Applications tab button.

   ii Select an application from the list and click on the Properties button. The Application (Edit) form opens with the General tab displayed.

   iii Click on the 5670 RAM Parameters tab button.

   iv Configure the Charging Group parameter.

   v Click on the OK button to close the Application (Edit) form.

vi Click on the Apply button in the AA Group Policy (Edit) form. A dialog box appears.

vii Click on the Yes button to save the changes.

7 Cloes the AA Group Policy (Edit) form.

Procedure 77-15 To configure application performance reporting on a service

Perform this procedure to enable application performance reporting on a service object and configure the default DCP subnet groups. Perform Procedure 77-16 to configure custom DCP subnet groups.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of services is displayed.

3 Select a service and click on the Properties button. The *service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the 5670 RAM Parameters tab button.

5 Configure the Enable Application Performance Reporting parameter.

6 Click on the Apply button to save the changes. Default Internet and Intranet DCP subnet groups are created within the VLL if you have enabled the Enable Application Performance Reporting parameter.

7 Configure statistics collection on the default DCP subnet groups, as required.

i Click on the Default DCP Groups tab button.

ii Choose the default Internet or Intranet DCP subnet group from the list and click on the Properties form. The Default DCP Group (Edit) form opens with the General tab displayed.

iii Configure the Collect Stats parameter.

iv Click on the OK button to save the changes and close the form.

8 Configure address rules on the default DCP subnet groups, as required.

i Click on the Default DCP Groups tab button.

ii Choose the default Internet or Intranet DCP subnet group from the list and click on the Properties form. The Default DCP Group (Edit) form opens with the General tab displayed.

iii Click on the Address Rules tab button.

iv Click on the Create button. The DCP Address Rule (Create) form opens.

v Configure the parameters:

- Auto-Assign ID
- ID
- Description
- IP Address Low
- High
- Mask

vi Click on the OK button to save the address rule and close the form.

vii Repeat steps iv to vi to add more address rules to the DCP subnet group, as required.

viii Click on the OK button to save the changes to the DCP subnet group and close the form.

9 Click on the Apply button in the *service_type* Service (Edit) form. A dialog appears.

10 Click on the Yes button.

11 Close the *service_type* Service (Edit) form.

Procedure 77-16 To configure a custom DCP subnet group

Perform this procedure to create a custom DCP subnet group for application performance reporting on a service and related objects. You must bind a custom DCP subnet group to one or more access interface objects and/or a spoke SDP binding in order to apply the customized DCP settings of the DCP subnet group.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of services is displayed.

3 Select a service and click on the Properties button. The *service_type* Service (Edit) form opens with the General tab displayed.

4 Click on the 5670 RAM Parameters tab button.

5 Click on the Custom DCP Groups tab button.

6 Click on the Create button. The Custom DCP Group (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Collect Stats

8 Associate the custom DCP subnet group with a SAP subscriber, if required.

i Click on the Select button in the SAP Subscriber panel. The Select SAP Subscriber - Custom DCP Group form opens.

ii Select a SAP subscriber and click on the OK button.

9 Associate the custom DCP subnet group with a spoke SDP binding subscriber, if required.

i Click on the Select button in the Spoke SDP Binding Subscriber panel. The Select Spoke SDP Binding Subscriber - Custom DCP Group form opens.

ii Select a spoke SDP binding subscriber and click on the OK button.

10 Associate the custom DCP subnet group with a transit subscriber, if required.

i Click on the Select button in the Transit Subscriber panel. The Select Transit Subscriber - Custom DCP group form opens.

ii Select a transit subscriber and click on the OK button.

11 Add address rules to the custom DCP subnet group, as required.

i Click on the Address Rules tab button.

ii Click on the Create button. The DCP Address Rule (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- IP Address Low
- High
- Mask

iv Click on the OK button to save the address rule and close the form.

v Repeat steps ii to iv to add more address rules to the DCP subnet group, as required.

12 Click on the OK button to save the custom DCP subnet group and close the form.

Custom DCP subnet groups are listed Custom DCP Group tab of the *service_type* Service form.

13 Click on the Apply button in the *service_type* Service form. A dialog appears.

14 Click on the Yes button to confirm the action and save the changes to the VLL service.

15 Close the *service_type* Service (Edit) form.

Procedure 77-17 To configure an AA HTTP error redirect policy

You must associate an AA HTTP error redirect policy with an AQP. See Procedure 77-3 for more information.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose one of the following:

a Create an AA HTTP error redirect policy:

i Click on the Create button and choose AA HTTP Error Redirect. The AA HHTP Error Redirect (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ISA-AA Group ID
- Displayed Name

iii Click on the Apply button. The form refreshes to display additional tabs and panels.

iv Go to step 3.

b Modify an AA HTTP error redirect policy:

i Choose AA HTTP Error Redirect (Application Assurance) from the object drop-down list.

ii Configure the filter criteria, if required, and click on the Search button. A list of AA HTTP Error Redirect policies is displayed.

iii Select a policy from the list and click on the Properties button. The AA HTTP Error Redirect (Edit) form opens with the General tab displayed.

iv Go to step 3.

3 Configure the parameters:

- Description
- Enabled
- HTTP Host
- Participant ID

4 Click on the Select button for the Template ID parameter. The Select Templated ID form opens.

5 Configure the filter criteria, if required, and click on the Search button. A list of templates is displayed.

6 Choose a template from the list and click on the OK button. The Template ID parameter is updated with the template ID.

7 To configure an HTTP error code, perform the following steps.

i Click on the HTTP Error Codes tab button.

ii Click on the Create button. The HTTP Redirect Error Code (Create) form opens.

iii Click on the Select button for the Redirect Error Code parameter. The Select Error Code form opens.

iv Configure the filter criteria, if required, and click on the Search button. A list of error codes is displayed.

v Choose an error code from the list and click on the OK button. The Redirect Error Code parameter is updated with the error code.

vi Configure the Message Size (octets) parameter, if required.

vii Click on the OK button. The error code is added to the list in the AA HTTP Error Redirect (Edit) form.

8 Click on the General tab button.

9 Click on the Switch Mode button. A dialog box appears.

10 Click on the Yes button.

11 Click on the More Actions button and choose Distribute to manually distribute the policy to one or more NEs. The Distribute - AA HTTP Error Redirect form opens.

12 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

13 Click on the Distribute button. The policy is distributed to the NEs.

14 Modify a local instance of the AA HTTP error redirect policy, if required.

i Click on the Local Definitions tab button. The AA HTTP error redirect policies for each managed NE are listed.

ii Choose an AA HTTP error redirect policy from the list and click on the Properties button to modify the local instance of the policy. The AA HTTP Error Redirect (Edit) form opens.

iii Click on the Switch Mode button.

iv Perform steps 3 to 10.

15 Click on the OK button. The AA HTTP Error Redirect (Edit) form closes and the Application Assurance Policies form reappears.

16 Close the Application Assurance Policies form.

Procedure 77-18 To configure AA protocol signatures

1 Choose Manage→ISA Functions→ISA-AA from the 5620 SAM main menu. The ISA-AA form opens.

2 Choose AA Protocol (Application Assurance) from the object drop-down list.

3 Specify a filter to create a filtered list of protocols, and click on the Search button. A list of protocols is displayed.

4 Select an entry in the list and click on the Properties button. The AA Protocol (Edit) form opens.

5 View the entry information.

6 Configure the Protocol Administrative State parameter, if required.

Note 1 — You can only configure the Protocol Administrative State parameter for a local protocol.

Note 2 — The Protocol Adminstrative State parameter is read-only for some protocols.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The AA Protocol (Edit) form closes and the ISA-AA form reappears.

9 Click on the Close button to close the ISA-AA form.

Procedure 77-19 To view AA summary information for subscribers, transit subscribers, SAPs, and spoke SDPs on ISA-AA MDAs

If the ISA-AA group is partitioned, the AA summary tabs appear on the partition. This information is typically used for AA debugging purposes. You can view debug statistics information on the Statistics tab of an AA object.

Caution — Alcatel-Lucent recommends that you consider the effect of resynchronizing an ISA-AA group. Resynchronizing an ISA-AA group typically involves the retrieval of an amount of information that is large enough to affect NE performance.

Note — You can view AA statistics using Stats Interval. Stats Interval allows you to choose realtime or snapshot for collecting AA statistics. Realtime specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, the statistics for any closed flows since the last collection window, and the statistics accumulated from any currently open flows. Snapshot specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to view AA summary information and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-AA Groups icon and click on the ISA-AA Group icon. The ISA-AA Group (Edit) form opens.

5 Click on the AA Summary tab button. The Subscribers, SAPs, Spoke SDP Bindings, and Transit Subscribers tabs are displayed.

6 Perform one of the following.

a View the summary information for a subscriber.

i Click on the Subscribers tab button. A list of subscribers is displayed.

ii Select an entry in the list and click on the Properties button. The AA Subscriber (Edit) form opens.

iii Click on the Properties button. The Residential Subscriber Instance (Edit) form opens.

b View the summary information for a SAP.

i Click on the SAPs tab button. A list of SAPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA SAP (Edit) form opens.

iii Click on the Properties button. The Access Interface (Edit) form opens.

c View the summary information for a spoke SDP.

i Click on the Spoke SDP Bindings tab button. A list of spoke SDPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA Spoke SDP Binding (Edit) form opens.

iii Click on the Properties button. The Spoke SDP Bindings (Edit) form opens.

d View the summary information for a transit subscriber.

i Click on the Transit Subscribers tab button. A list of transit subscribers is displayed.

ii Select an entry in the list and click on the Properties button. The AA Transit Subscriber (Edit) form opens.

iii Click on the Properties button. The Transit Subscriber (Edit) form opens.

7 Click on the Statistics tab button.

8 Choose an AA statistics class from the object drop-down list.

9 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

10 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

11 View the statistics data.

12 Close the Statistics Record form.

13 Close the subscriber, SAP, or spoke SDP properties forms.

Procedure 77-20 To view the AA special study statistics data

Perform this procedure to view the AA special study statistics data for subscribers, transit subscribers, SAPs, or spoke SDPs on an ISA-AA MDA. If the ISA-AA group is partitioned, the AA special study tabs appear on the partition.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to view AA special study statistics data and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-AA Groups icon and click on the ISA-AA Group icon. The ISA-AA Group (Edit) form opens.

5 Click on the AA Special Study tab button. The Subscribers, SAPs, Spoke SDP Bindings, and Transit Subscribers tabs are displayed.

6 Perform one of the following.

a View the special study statistics for a subscriber.

i Click on the Subscribers tab button. A list of subscribers is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study Subscriber Config (Edit) form opens.

iii Click on the Properties button. The Subscriber (Edit) form opens.

b View the special study statistics for a SAP.

i Click on the SAPs tab button. A list of SAPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study SAP Config (Edit) form opens.

iii Click on the Properties button. The Access Interface (Edit) form opens.

c View the special study statistics for a spoke SDP.

i Click on the Spoke SDP Bindings tab button. A list of spoke SDPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study Spoke SDP Binding Config (Edit) form opens.

iii Click on the Properties button. The Spoke SDP Binding (Edit) form opens.

d View the special study statistics for a transit subscriber.

i Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers list form opens.

ii Specify a filter to create a filtered list of transit subscribers, and click on the Search button. A list of transit subscribers is displayed.

iii Select an entry in the list and click on the Properties button. The Database Persisted Transit Subscriber form opens with the General tab displayed.

7 Click on the Statistics tab button.

8 Choose an AA statistics class from the object drop-down list.

9 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

10 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

11 View the statistics data.

12 Close the Statistics Record form.

13 Close the subscriber, SAP, or spoke SDP forms.

Procedure 77-21 To view AA statistics data for ISA-AA groups or ISA-AA partitions

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to view AA statistics data and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 On the Network Element (Edit) form navigation tree, expand the Logical Groups icon.

4 Expand the ISA-AA Groups icon and click on the ISA-AA Group icon. The ISA-AA Group (Edit) form opens with the General tab button displayed.

5 Perform one of the following:

   a View AA statistics data for an ISA-AA group.

      i Click on the Statistics tab button.

      ii Choose an AA statistics class from the object drop-down list.

   b Perform the following steps to view AA statistics data for an ISA-AA partition.

      i Click on the ISA-AA Partitions tab button. A list of ISA-AA partitions is displayed.

      ii Select an entry in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens with the General tab button displayed.

      iii Click on the Statistics tab button.

      iv Choose an AA statistics class from the object drop-down list.

6 Perform one of the following:

   a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

   b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

7 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

8 View the statistics data.

9 Close the Statistics Record form.

10 Close the ISA-AA forms.

Procedure 77-22 To view AA statistics data for application filters

You can view application filter hit counts on local definitions of AA group policies.

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list.

3 Configure the filter criteria, if required, and click on the Search button. A list of AA group policies is displayed.

4 Select an AA group policy from the list and click on the Properties button. The AA Group Policy - Global Policy (Edit) form opens with the General tab displayed.

5 Click on the Local Definitions tab button.

6 Configure the filter criteria, if required, and click on the Search button. A list of local AA group policy definitions is displayed.

7 Select a local AA group policy from the list and click on the Properties button. The AA Group Policy - Local Policy (Edit) form opens with the General tab displayed.

8 Click on the Application Filters tab button.

9 Configure the filter criteria, if required, and click on the Search button. A list of NE application filters is displayed.

10 Select an application filter from the list and click on the Properties button. The Application Filter - Local Policy (Edit) form opens with the General tab displayed.

11 Click on the Statistics tab button.

12 Click on the Collect All button.

13 Click on the Search button. A list of collected statistics is displayed.

14 Select a statistics object from the list and click on the Properties button. The Statistics Record - AA Application Filter Stats form opens.

15 View the statistics data.

16 Close the Statistics Record - AA Application Filter Stats form.

17 Close the Application Filter - Local Policy (Edit) form.

18 Close the AA Group Policy - Local Policy (Edit) form.

19 Close the AA Group Policy - Global Policy (Edit) form.

20 Close the Application Assurance Policies form.

Procedure 77-23 To delete an AA application, application group, or custom protocol

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select a policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Delete an AA application.

i Click on the Applications tab button. A list of AA applications is displayed.

ii Choose an application in the list and click on the Delete button. A warning form appears.

iii Click on the View Dependencies button.

Note — When the AA application is on a global AA group policy, the counts include all of the dependencies on the global and local NEs. When the AA application is on a local AA group policy, the counts include all of the dependencies on the local NE only.

b Delete an application group.

i Click on the Application Groups tab button. A list of application groups is displayed.

ii Choose an application group in the list and click on the Delete button. A warning form appears.

iii Click on the View Dependencies button.

Note — If the application group is on a global AA group policy, the counts include all of the dependencies on the global and local NEs. If the application group is on a local AA group policy, the counts include all of the dependencies on the local NE only.

c Delete a custom protocol.

i Click on the Custom Protocols tab button. A list of custom protocols is displayed.

ii Choose a custom protocol in the list and click on the Delete button. A warning form appears.

iii Click on the View Dependencies button.

Note — If the custom protocol is on a global AA group Policy, the counts include all of the dependencies on the global and local NEs. If the custom protocol is on a local AA group policy, the counts include all of the dependencies on the local NE only.

5 Review the dependencies and click on the OK button.

6 Select the I understand the implications of this action check box.

7 Click on the Yes button, and then click on the OK button. The AA Group Policy (Edit) form appears.

8 Click on the Apply button, and then click on the Yes button.

9 If you deleted an AA application, application group, or custom protocol on a global AA group policy, you must distribute the changes to the local AA Group Policy. Go to step 10, otherwise, go to step 13.

10 Click on the General tab button.

11 Click on the Switch Mode button. A dialog box appears.

12 Click on the OK button.

13 Close the AA Group Policy (Edit) form.

Procedure 77-24 To delete an AA transit subscriber

Use this procedure to remove the record of an inactive AA transit subscriber from the 5620 SAM database. AA transit subscribers become inactive in the 5620 SAM when the subscriber is deleted from the AA transit IP policy.

Note 1 — Use a size constraint policy to ensure that the number of inactive AA transit subscribers in the 5620 SAM database remains at a manageable level. See chapter 61 for more information.

Note 2 — AA statistics data can be lost when you delete an AA transit subscriber instance before the 5620 SAM is finished collecting and processing AA statistics. Alcatel-Lucent recommends waiting at least two statistics collection intervals before deleting an inactive AA transit subscriber instance.

1 Choose Manage→AA Transit Subscribers from the 5620 SAM main menu. The Manage AA Transit Subscribers form opens.

2 Configure the filter criteria and click on the Search button. A list of AA transit subscribers appears.

The Active property indicates the status of each AA transit subscriber in the list. An inactive AA transit subscriber instance has no check mark under the Active heading.

3 Select the inactive AA transit subscriber you want to delete and click on the Delete button. The inactive AA transit subscriber instance is removed from the list.

4 Close the Manage AA Transit Subscribers form.

78 — Service Test Manager

78.1 Service Test Manager overview

The 5620 SAM service test manager (STM) provides the ability to group various OAM tests into test suites for network troubleshooting and for verifying compliance with SLAs. You can schedule the execution of a test suite to provide continual performance feedback, or run a test suite on demand to investigate service issues. The test results are logged for monitoring and trend analysis.

The grouping of tests into a test suite allows a 5620 SAM operator to use one schedule for the periodic execution of multiple OAM diagnostics against multiple network objects; for example, services, NEs, or transport components. An operator can choose to include existing tests, use the 5620 SAM to generate the tests that comprise a test suite, or both. Groups of tests in a suite can be configured to execute sequentially or concurrently. In addition, you can configure a test suite as an OAM validation test to verify the operational status of a service.

You can configure threshold-crossing parameters to generate alarms when rising or falling threshold values are reached due to the reach, latency, or jitter issues discovered by the OAM tests.

The 5620 SAM STM allows the deployment of the maximum number of tests to a 7450 ESS or 7750 SR. The 5620 SAM raises an alarm when the number of tests on an NE is 60% of the configured maximum. Attempts to create or execute a test using the 5620 SAM fail when the number of deployed tests on an NE is too high.

Test policies

To enable the automatic generation of tests for a test suite, the 5620 SAM requires a test policy that contains a set of test definitions and pre- and post-processing rules. A test policy also specifies the order of execution for the generated tests. A test policy applies to only one test suite, and a test suite can have only one associated test policy.

Test policy parameters can be configured to display test results only if a test fails or generates a threshold crossing alarm. In large networks, this can substantially reduce the amount of test data that the 5620 SAM needs to collect.

A test policy is specific to one type of entity; for example, a VLL service or service tunnel. The test definitions in the policy are restricted to the tests that apply to the entity type specified in the policy. A test policy is applied to a test suite during test suite creation.

Test suites

A test suite contains three test groups:

- **First-run tests**
  First-run tests are the tests in a suite that the 5620 SAM executes before the tests in the other groups. First-run tests are chosen from a list of existing tests and might typically include high-level diagnostics; for example, a service site ping or VPRN ping. No restrictions apply to the types of tests that are selectable as first-run tests.

- **Generated tests**

  Generated tests are created by the 5620 SAM for use against a specific network entity, based on the entity type specified in the suite and the specific tested entities that are named in the associated test policy. For example, a service site ping test policy associated with a three-site VPRN test suite causes the 5620 SAM to generate six tests: one site ping test from each site in the VPRN to the other two sites. When you change the configuration of a network entity, such as a service, you must regenerate the generated tests that apply to the entity. Test regeneration removes previously generated tests from a test suite.
- **Last-run tests**

  Last-run tests are the tests in a suite that the 5620 SAM executes after the tests in the other groups. Last-run tests are chosen from a list of existing tests and might typically include transport-layer diagnostics; for example, an LSP trace or a tunnel ping. No restrictions apply to the types of tests that are selectable as last-run tests.

To create a test suite that contains tests for different entity types, you can specify that the test suite applies to no specific entity type. In this way, you can create a group of disparate tests to which no test policy restrictions apply. Specifying none as the entity type in a test suite has the following effects.

- It allows you to choose any predefined test as a first-run or last-run test.
- It disables test generation in the test suite, because test generation requires a test policy that is based on a specific entity type.

Note — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on an NE, for example, using a CLI.

To manage the system resources that test execution consumes, the 5620 SAM assigns a weight value to a test. When the 5620 SAM executes a test, it attempts to reserve the test weight from a resource pool, performs the test, then returns the test weight to the pool. The weight of a test suite is the sum of the weights of the individual tests in the suite. The 5620 SAM attempts to reserve the weight of the whole suite for the duration of suite execution. If the required weight for a test or test suite is unavailable, execution is halted and the Status value contained in the test result is set to Not Enough Resources.

You can create an OAM service validation test to verify the operational status of a service. The operational status of a service depends on the operational states of its service sites or instances. It is possible for a service to be operationally up when communication between sites is not operational. For example, a VRF can be operationally up but the routes to its peers might not be populated because of the routing policy, route target, or ACL configuration. The State Cause of the service indicates the success or failure of the OAM validation test, and therefore, service connectivity.

You can configure an OAM validation test when you create a test suite and run the OAM validation test from the service configuration form.

Note — OAM validation tests are not supported for HVPLS.

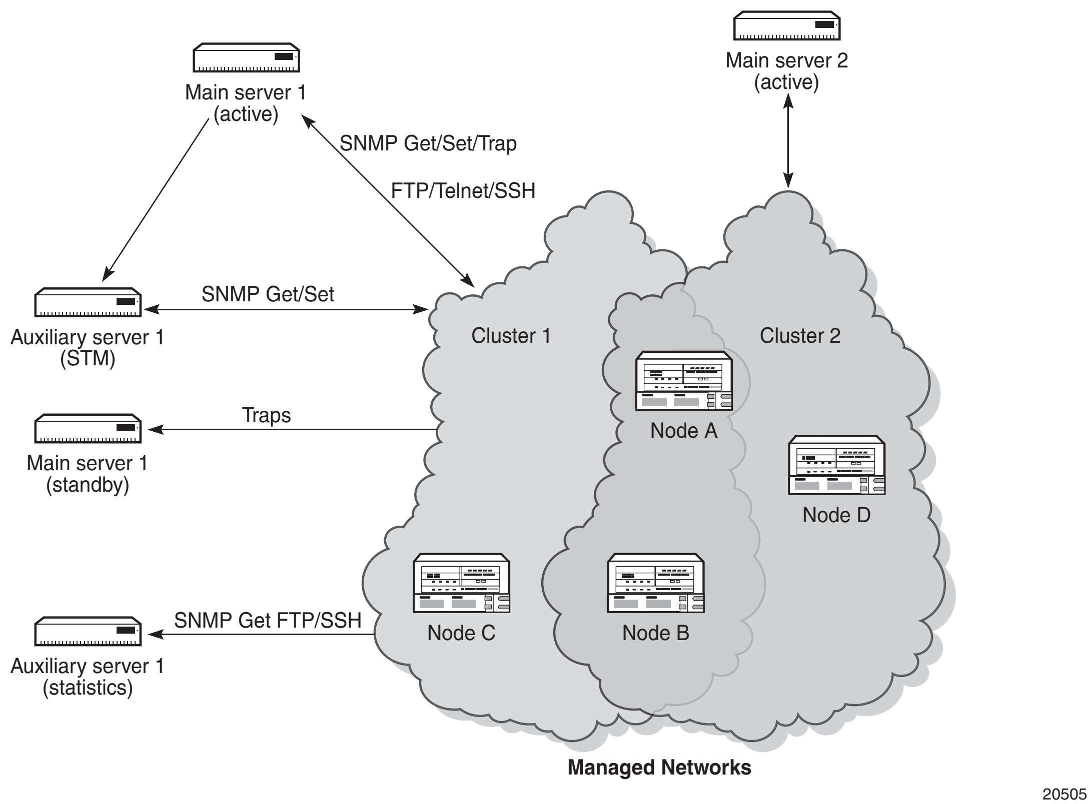
Consider the following when you create or execute test suites.

- A test, whether pre-existing or generated, is associated with only one test suite.
- You can execute a generated test on demand, not just in the context of a test suite.
- STM test suites can be configured as scheduled tasks. See chapter 79 for information about using the 5620 SAM to schedule tasks.
- Using an NE schedule does not ensure that the target NEs perform the actions in an associated STM scheduled task in the order specified; the NEs that execute an NE scheduled task operate independently and are not directed by the 5620 SAM. As soon as an NE completes an action in an NE scheduled task, it performs the next action.
- The 5620 SAM database logs test results only for scheduled test suites that are associated with SAM schedules. Logging for test suites that are associated with NE schedules is performed locally on each target NE.
- Size constraint policies control the number of historical records that the 5620 SAM retains in the database. You can configure size constraint policies to limit the number of database objects that are associated with specific test types. See chapter 46 for information about size constraint policies.
- A 5620 SAM user that is assigned the admin or QoS/ACL management scope of command role can create and modify all tests, test policies, and test suites. A user that is assigned the service management scope of command role can create and modify only STM components that are related to services. A user that is assigned the topology management role can create and modify only STM components that are related to network transport elements.
- OAM test suites in which the Validation Test Suite parameter is enabled are used to test the operational status of a service or service-related entity such as a service tunnel. The result of the test is indicated by the OAM Validation Failed state cause indicator on the General tab of the management form for the object.
- You can view test-suite results for an object from the Tests tab of the configuration form for the object.

OAM test ID ranges

You can configure a test ID for the OAM tests in multiple server environments. A test ID allows you to identify the source server that initiated the OAM test. Figure 78-1 shows an example of a network configuration on which a user could run OAM tests on Node A and Node B from the 5620 SAM main 1 or main 2 servers. In this example, Node A and Node B are members of two network clusters that are managed by separate 5620 SAM servers, Main server 1 (active) and Main server 2 (active).

Figure 78-1 Multiple STM implementation



You can execute OAM tests from the new main server after a redundancy switch from Main server 1 (active) tom Main server 1 (standby).

You can configure the nms-server.xml file to configure the range for the test IDs. You must use the same ID range for the 5620 SAM main and standby servers that are managing a distinct network cluster. The OAM tests always have a test ID in the specified range.

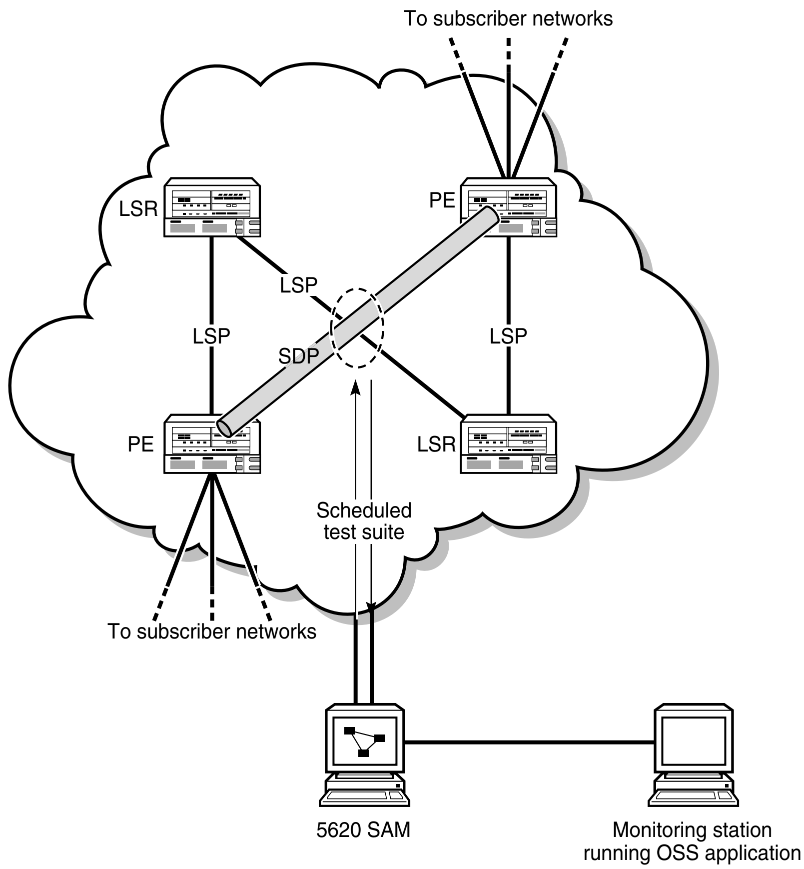
The 5620 SAM does not validate the range values for the test IDs. However, the 5620 SAM raises a major alarm upon receipt of a test with a test ID outside the range, or when the range is changed in the nms-server.xml file.

See Procedure 78-1 for info on how to change the test ID range.

78.2 Sample Service Test Manager implementation

Figure 78-2 shows a sample STM implementation that illustrates how you can use STM suites to verify service operation and identify network problems.

Figure 78-2 Sample STM implementation



In the sample network, two scheduled STM test suites run constantly to ensure that the transport elements are functioning properly. One test suite monitors the SDPs, and the other test suite monitors the LSPs. A 5620 SAM administrator can quickly update the test suites, as required, to reflect network topology changes by revising the list of tested entities in the suite and regenerating the tests. An OSS application collects the test result information which is then available for monitoring by NOC staff.

Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 79 for information about SAM schedules.

The SDP test suite contains the following generated tests for each SDP:

- tunnel ping
- MTU ping

The LSP test suite contains the following generated test for each LSP path:

- LSP ping (tested entity type is LSP path)

NOC monitoring staff become aware that tunnel ping operations fail occasionally on one SDP. Packet loss is not yet significant enough to affect SLAs, but threatens to become so, based on the observed trend. NOC staff run a test suite against the LSPs in the affected LSP path. The test suite contains the following generated test for each LSP in the LSP path:

- LSP ping (tested entity type is LSP)

Test results show that the packet loss is related to a specific LSP in the path. Investigation of the LSP traffic pattern indicates that a recently provisioned service is causing the LSP to be oversubscribed. The problem is addressed by a network designer and is corrected through configuration changes.

Table 78-1 lists the high-level tasks necessary to configure and use the STM elements in this sample.

Table 78-1 Sample STM implementation configuration sequence

Task	Description
1. Scheduled STM test-suite creation	Create STM test policies for transport-layer elements. • Create a test policy for the SDPs. Specify Tunnel (SDP) as the Entity Type for the policy, and choose Tunnel Ping and MTU Ping as the test definitions. Create separate tunnel ping definitions for different forwarding classes, as required. • Create a test policy for the LSP paths. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP Path as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create STM test suites for transport-layer elements. • Create a test suite for the SDPs. Specify Tunnel (SDP) as the Entity Type for the suite, choose the SDP test policy, choose the SDPs against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task. • Create a test suite for the LSP paths. Specify LSP as the Entity Type for the suite, choose the LSP test policy, choose the LSP paths against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task.
2. Data presentation	Customize the tabular display of test results in the 5620 SAM, or create an OSS application that retrieves test-result data from the 5620 SAM and presents it as information in graphical format for NOC staff.
3. Creation of non-scheduled STM test suite or individual OAM tests for network troubleshooting	Create an STM test policy for the LSPs for use during network troubleshooting. • Create a test policy for the LSPs. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create a non-scheduled STM test suite (or individual OAM tests, depending on the number of LSPs involved) for the LSPs in the LSP path. • Specify LSP as the Entity Type for the suite, choose the newly created LSP test policy, choose the LSPs in the LSP path against which the suite is to run, and use the 5620 SAM to generate the tests for the suite.
4. Network monitoring	Use the 5620 SAM to display the scheduled test results in tabular format, or use an OSS application to monitor the LSP ping, tunnel ping, and MTU ping diagnostic results in real time. Record inconsistencies and trends, and troubleshoot the network as required. Use the threshold-crossing alarm capabilities to raise alarms when traffic characteristics rise above or fall below specific values.

(1 of 2)

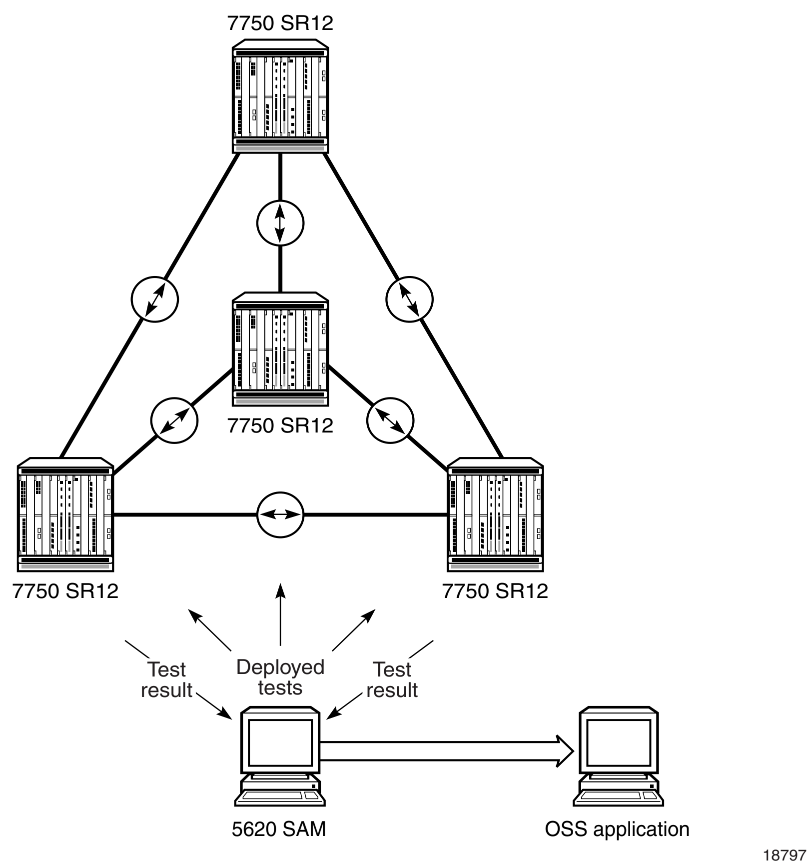
Task	Description
5. Network troubleshooting	When potential trouble arises, use a non-scheduled STM test suite or individual STM tests to help identify the cause. • Create individual tests or edit the existing non-scheduled test suite. Include as tested entities the LSPs that comprise the LSP path and regenerate the tests for the suite, as required. • Execute the non-scheduled test suite and monitor the test results. • Edit the test definition in the test policy. Change test parameter values as required, regenerate the tests in the suite, and re-execute the suite. Continue to refine the diagnostic test results until the problem manifests itself in the test results.

(2 of 2)

78.3 Sample network monitoring configuration

Figure 78-3 shows the high-level flow of tests and test results in a simple network topology that the network provider wants to continually monitor using the STM. See section 78.4 for the explicit steps required to create the STM configuration.

Figure 78-3 Continual network topology monitoring



A 5620 SAM administrator creates and schedules an STM test suite to monitor the LSP mesh and identify potential overloading and reachability problems before they affect service traffic. The test suite contains ping and trace test definitions for three different classes of in-profile traffic and is scheduled to run every 15 minutes.

Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 79 for information about SAM schedules.

Because the same group of tests is to be run on multiple entities of the same type, the test suite consists of generated tests only. The test policy that the 5620 SAM uses to generate the tests contains the following six test definitions:

- LSP ping - be in
- LSP ping - af in
- LSP ping - nc in
- LSP trace - be in
- LSP trace - af in
- LSP trace - nc in

The 5620 SAM generates 72 tests for the test suite—3 ping tests and 3 trace tests for each of the 12 LSPs and LSP paths. Every 15 minutes, the 5620 SAM scheduler executes the tests and stores the results. An OSS application periodically retrieves the test results, performs trend analysis and presents the transport utilization information to NOC monitoring staff.

The 5620 SAM generates an alarm in the event of an LSP ping probe failure or an LSP trace path change, as specified in the test policy, so 5620 SAM operators become aware of new transport faults as they arise.

78.4 Sample network monitoring configuration steps

The following steps explicitly define the end-to-end configuration of the network monitoring sample in section 78.3. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 78.11 for complete STM configuration information.

Create test policy for test generation

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4 Configure the parameters in Table 78-2 using the supplied values:

Table 78-2 Test policy General tab parameters

Parameter	Value	Comment
Name	LSP Test Policy	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.
Entity Type	LSP	—

5 Click on the Test Definitions tab button.

6 Click on the Add button to add a test definition to the test policy. A menu appears.

7 Choose MPLS→Add LSP Ping. The LSP Ping Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Ping test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

8 Configure the parameters in Table 78-3 using the supplied values, most of which are common to the three test definitions:

Table 78-3 LSP Ping Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Ping - be in LSP Ping - af in LSP Ping - nc in	First test definition Second test definition Third test definition
Target Type	LSP	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and version of device against which a test runs.
Forwarding Class	be af nc	For LSP Ping - be in test definition For LSP Ping - af in test definition For LSP Ping - nc in test definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses three LSP ping definitions that differ only by forwarding class.
Forwarding Profile	in	All test packets are marked in-profile. This means that they follow the same path as service traffic.

(1 of 2)

Parameter	Value	Comment
Results configuration tab		
Probe History Size (rows)	100	—
Trap Generation	Probe Failure	Test-probe failures provide early notification of LSP congestion or reachability issues to a 5620 SAM operator. OSS analysis of the results indicates trends for further investigation.

(2 of 2)

9 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

10 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

11 Repeat steps 6 to 10 for the remaining test definitions listed in step 7.

12 Click on the Add button to add a test definition to the test policy. A menu appears.

13 Choose MPLS→Add LSP Trace. The LSP Trace Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Trace test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

14 Configure the parameters in Table 78-4 using the supplied values. Values that are not common to the three test definitions are so indicated.

Table 78-4 LSP Trace Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Trace - be in LSP Trace - af in LSP Trace - nc in	For first test definition For second test definition For third test definition
Target Type	LSP Path	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and version of device against which a test runs.

(1 of 2)

Parameter	Value	Comment
Forwarding Class	be af nc	For LSP Trace - be in definition For LSP Trace - af in definition For LSP Trace - nc in definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses a different LSP ping definition for each forwarding class.
Forwarding Profile	in	All LSP ping test definitions in the sample involve in-profile traffic.
Results configuration tab		
Probe History Size (rows)	100	—
Trap Generation	Test Failure Path Change	A test failure trap may indicate a routing or congestion issue, but it also indicates test misconfiguration when the Maximum Time to Live parameter value is too low to allow a test probe to reach the destination LSP. A path change trap may indicate an intermittently congested or unresponsive LSP.

(2 of 2)

15 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

16 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

17 Repeat steps 12 to 16 for the remaining test definitions listed in step 13.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create schedule

20 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

21 Click on the Create button and choose Create SAM Schedule. The SAM Schedule (Create) form opens.

22 Configure the parameters in Table 78-5 using the supplied values:

Table 78-5 SAM Schedule parameters

Parameter	Value	Comment
Name	LSP Assurance	—

(1 of 2)

Parameter	Value	Comment
Current Client Start Time	a future time	Specify the date and time at which the schedule is to be first triggered. This value is used to calculate the times of subsequent triggers, based on the Frequency parameter value. Compare this value and the Frequency parameter value with those in other 5620 SAM schedules to ensure that the schedule trigger times are staggered and the resulting NE task load is balanced.
Ongoing	enabled	This setting tells the 5620 SAM to continually trigger execution of the task associated with the schedule.
Frequency	Per Minute / 15	You must also select the Run Every Minutes radio button and specify 15 as the number of minutes for the triggering frequency.

(2 of 2)

23 Click on the OK button. The SAM Schedule (Create) form closes.

24 Close the Schedule form.

Create test suite

25 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

26 Configure the parameters in Table 78-6 using the supplied values.

Table 78-6 Test suite parameters

Parameter	Value	Comment
Name	LSP Test Suite	—
Entity Type	LSP	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.

27 Click on the Test Policy tab button.

28 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

29 Configure the filter properties and click on the Search button. A list of test policies is displayed.

30 Select the LSP Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

31 Click on the Tested Entities tab button.

32 Click on the Add button to choose the LSPs that are to be regularly assessed by the test suite. The Select Tested Entity - Test Suite form opens.

33 Configure the filter properties and click on the Search button to display a list of LSPs.

34 Select the LSPs that you want to include and click on the OK button. The LSPs are listed on the Test Suite (Create) form.

35 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

36 Click on the Generated Tests tab button.

37 Click on the Generate Tests button. The 5620 SAM generates a test for each LSP listed on the Tested Entities tab. The tests are listed on the form as they are generated.

Apply a span of control to a test suite

38 Click on the Spans tab button.

39 Click on the Add button. The Select Spans - Test Suite form opens with a list of available spans.

40 Select one or more spans to apply to the test suite.

41 Click on the OK button. The Select Spans - Test Suite form closes and a dialog box appears.

42 Click on the OK button to confirm the action.

Create scheduled task

43 Click on the Schedule button and choose Create SAM Scheduled Task. The SAM Scheduled Task (Create) form opens with LSP Test Suite displayed in the Task panel.

44 Configure the parameters in Table 78-7 using the supplied values.

Table 78-7 SAM scheduled task parameters

Parameter	Value	Comment
Scheduled Task Name	Periodic LSP Check	—
Administrative State	Enabled	The 5620 SAM executes the scheduled task at regular intervals based on the specified Current Client Start Time and Frequency.

45 Click on the Select button. The Select Schedule - SAM Scheduled Task form opens.

46 Select LSP Assurance and click on the OK button. The 5620 SAM automatically populates the Schedule panel with the schedule information.

47 Click on the OK button. The SAM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

48 Close the Test Suite (Edit) form.

49 Close the Service Test Manager form.

78.5 Sample SAA accounting files configuration

The following sample configuration focuses on the configuration of SAA accounting files that are to be collected following the generation of an NE schedulable test of VLL services.

A network provider wants to use the 5620 SAM to view test result information for a NE schedulable test of VLL services and wants the 5620 SAM to process the OAM results MIB entries and produce a compressed XML record that is stored in SAA accounting files on the nodes.

A 5620 SAM administrator must create an NE schedulable test for VLL services that records test result information in SAA accounting files. The administrator creates one accounting policy, one file policy, one test policy, and one test suite. Section 78.6 describes the steps that are required to create a test.

78.6 Sample SAA accounting files configuration steps

The following steps explicitly define the end-to-end configuration of the SAA accounting files sample in section 78.5. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 78.11 for complete STM configuration information.

Create accounting policy

1. Choose Tools→Statistics→Accounting Policies from the 5620 SAM main menu. The Manage Accounting Policies form opens.

2. Click on the Create button. The Accounting Policy (Create) form opens.

3. Configure the parameters in Table 78-8 using the supplied values.

Table 78-8 Accounting policy parameters

Parameter	Value	Comment
Displayed Name	SAA Accounting Policy	—
Type	NE Schedulable Tests	You must choose this value to allow the configuration of SAA accounting files

4. Click on the Select button beside the File ID parameter. The Select A File Policy form opens.

5. Click on the Create button. The File Policy (Create) form opens.

6. Configure the Displayed Name parameter. For the purposes of this sample, the value shall be SAA File Policy.

7. Click on the OK button. The File Policy (Create) form closes and the Select A File Policy form reappears.

8. Select the SAA File Policy entry and click on the OK button. The Select A File form closes and the file policy is listed on the Accounting Policy (Create) form.

9 Click on the OK button. The Accounting Policy (Create) form closes and the Manage Accounting Policies form reappears.

10 Configure the filter properties and click on the Search button. A list of accounting policies is displayed

11 Select the SAA Accounting Policy entry and click on the Distribute button. The Distribute form opens.

12 Select the entities that you want to include and click on the OK button. The Distribute form closes.

13 Close the Manage Accounting Policies form.

Create test policy

14 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

15 Click on the Create button.

16 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

17 Configure the parameters in Table 78-9 using the supplied values:

Table 78-9 Test policy parameters

Parameter	Value	Comment
Name	SAA Test Policy	—
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.
Entity Type	VLL Service	—
Accounting Files	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

18 Click on the Test Definitions tab button.

19 Click on the Add button to add a test definition to the test policy. A menu appears.

20 Choose Service→Add VCCV Ping. The VCCV Ping Definition (Create) form opens with the General tab displayed.

21 Click on the OK button. The VCCV Ping Definition (Create) form closes and a dialog box appears.

22 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

23 Click on the OK button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create test suite

24 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

25 Configure the parameters in Table 78-10 using the supplied values:

Table 78-10 Test suite parameters

Parameter	Value	Comment
Name	SAA Test Suite	—
Entity Type	VLL Service	—
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

26 Click on the Test Policy tab button.

27 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

28 Configure the filter properties and click on the Search button. A list of test policies is displayed.

29 Select the SAA Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

30 Click on the Tested Entities tab button.

31 Click on the Add button. The Select Tested Entity - Test Suite form opens.

32 Configure the filter properties and click on the Search button to display a list of entities.

33 Select the nodes that were used in step 12 and click on the OK button. The nodes are listed on the Test Suite (Create) form.

34 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

35 Click on the Generated Tests tab button.

36 Click on the Generate Tests button. The 5620 SAM generates a test for each entity listed on the Tested Entities tab. The tests are listed on the form as they are generated.

78.7 Sample threshold-crossing alarm configuration

The following sample configuration focuses on the configuration of a threshold-crossing alarm that is to be included in a test suite. It does not describe the configuration of the test suite, schedule or scheduled task associated with the sample. No test policy is required for the configuration, as it does not involve generated tests.

A network provider wants to use the 5620 SAM to monitor a customer VPLS named VPLS 17 that carries VoIP traffic. He wants the 5620 SAM to raise an alarm when the round-trip jitter value rises above a specified threshold.

Network jitter values typically range from 10 to 15 ms, but are occasionally as high as 25 ms. Jitter buffers in the end-user VoIP sets can accommodate up to 80 ms of jitter. A network engineer determines that a jitter test threshold of 30 ms is low enough to allow NOC operators sufficient time for investigating a jitter increase, yet high enough to exclude spurious jitter events.

A 5620 SAM administrator wants to creates a scheduled CPE ping test suite for the VPLS that periodically measures the round-trip jitter between each VPLS site and an end device. The administrator creates one CPE ping test for each site in the VPLS. Section 78.8 describes the steps required to create one such test.

78.8 Sample threshold-crossing alarm configuration steps

The following procedure explicitly defines the configuration steps required to create the test with a threshold-crossing alarm described in section 78.7. See section 78.4 for information about sample test-suite, test policy, or scheduling configurations. See the procedures in section 78.11 for complete STM configuration information.

For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample.

Create CPE ping test with threshold-crossing criteria

1 Click on the Create button in the Service Test Manager form and choose L2 Service→CPE ping from the contextual menu. The CPE Ping Test (Create) form opens with the General tab displayed.

2 Configure the parameters in Table 78-11 using the supplied values:

Table 78-11 General CPE Ping test parameters

Parameter	Value	Comment
General tab		
Name	CPE Ping Test - VPLS 17, Site A	A descriptive name such as this is helpful for quickly identifying the entity under test when viewing the test results.
NE Schedulable	enabled	You must enable this parameter to allow the configuration of threshold-crossing criteria.
Select button in Service panel	VPLS 17	Click on the Search button on the Select Service - CPE Ping form that opens to choose a service.
Select button in Site panel	Site A	Click on the Search button on the Select Site - CPE Ping form that opens to choose a service.
Destination Path Address	*IP address of an end device connected to Site A*	This is the IP address to which the CPE ping packets are sent.
Source IP Address	*IP address of the NE that originates the test packets*	This IP address must be in the same subnet as the Destination IP Address.

(1 of 2)

Parameter	Value	Comment
Source MAC Address	*MAC address of the NE that originates the test packets*	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Results configuration tab		
Probe History Size (rows)	100	This value provides a greater retained test-result history for occasional monitoring by a 5620 SAM operator.
Trap Generation	Probe Failure	Test-probe failures provide early notification of congestion or reachability issues to a 5620 SAM operator for troubleshooting purposes.

(2 of 2)

3 Click on the Apply button. Additional buttons and tab buttons appear, and the form name changes to CPE Ping *Test Name* (Edit).

4 Click on the Threshold Alarms tab button.

5 Click on the Add button to add threshold criteria. The NE Threshold Event (Create) form opens with the General tab displayed.

6 Configure the parameters in Table 78-12 using the supplied values:

Table 78-12 Threshold-crossing CPE Ping test parameters

Parameter	Value	Comment
Type	Round-Trip Jitter	—
Generate Alarm on Rising Threshold	enabled	This is the default setting. Alternatively or additionally, by enabling the Generate Alarm on Rising Threshold parameter, you can configure the 5620 SAM to generate an alarm when a test-result value falls below a specified threshold. You can also configure the 5620 SAM to clear a rising-threshold alarm when the test-result value falls below the value configured for the falling threshold.
Rising Threshold tab		
Threshold Value	30	This value specifies that the 5620 SAM is to generate an alarm when an individual test result contains a round-trip jitter value greater than 30 ms.

7 Click on the OK button. The NE Threshold Event (Create) form closes.

8 Close the CPE Ping *Test Name* (Edit) form.

78.9 Sample OS 6250M (Metro) device SLA testing

You can use the 5620 SAM STM to perform a CPE SLA Test-Head OAM test to validate and test customer SLAs used on OS 6250M devices in Metro Ethernet networks. The test is critical for provisioning or troubleshooting network services between customer endpoints. The CPE SLA Test-Head OAM test supports unidirectional traffic and IPv4.

You can perform the following tasks on the 5620 SAM without an external test-head device:

- Generate specific flow-based traffic across the network to help identify flow-based issues.
- Identify the impact of QoS settings (for example, SAP profile or QoS policies) on the overall traffic.
- Check the throughput across a provider network. The throughput is displayed on the 5620 SAM GUI for each iteration of the test.
- Debug flow-specific traffic forwarding across the provider network.
- Analyze the behavior of various user-defined traffic patterns across the provider network.
- Perform the handover testing after the initial deployment.
- Perform on-demand testing and results monitoring using a central entity.

You can perform a CPE SLA Test-Head test using one CPE test-head profile or a group of profiles. You can also run several tests for one CPE Test-Head profile or group of profiles.

The following conditions are applicable to the creation of a CPE SLA Test-Head profile or a group of profiles and their execution:

- A CPE SLA Test-Head Group profile can contain up to eight stream/flows.
- A CPE SLA Test-Head Group profile can contain up to eight analyzers.
- When you configure the STM test execution details, the analyzer test name and the generator test name must be the same.
- If the analyzer has a test (flow) which is not in the generator group profile, the test is not valid.
- When you run a CPE SLA test or test group, only one test can be run at a time. You cannot run concurrent tests on the same OS 6250M device.

The following steps describe how to create a CPE SLA Test-Head profile or a group of profiles (OS 6250M [Metro] devices only). The procedure lists only the configuration steps and parameters that are required for the sample. See the procedures in section 78.11 for complete STM configuration information.

Create a CPE SLA Test-Head profile

1 Choose Tools→AOS CPE Test-Head Profiles→CPE Test-Head Profile from the 5620 SAM main menu. The CPE Test-Head Profiles form opens.

2 Click on the Create button. The CPE Test-Head Profile, Global Policy (Create) form opens.

3 Configure the following parameters:

- Name
- Description
- Source Endpoint
- Destination Endpoint
- Source MAC
- Destination MAC
- Direction
- Role
- Tx Rate (kbps)
- Frame Size (bytes)

4 Configure the Frame Type parameter. The CPE Test-Head Profile, Global Policy (Create) form refreshes and displays additional parameters.

5 Configure the following parameters:

- VLAN-Tag
- Priority
- Pattern
- Drop Enable

6 Perform one of the following:

a If you set the Frame Type parameter to Ethernet, configure the Ether Type parameter.

b If you set the Frame Type parameter to IPV4, configure the following parameters.

- Source IP
- Destination IP
- Protocol
- TOS
- TTL
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear when you set the Protocol parameter to TCP or UDP.

7 Click on the OK button. The CPE Test-Head Profiles form opens.

8 Click on the Search button to display the CPE Test-Head profile.

9 Choose the CPE Test-Head profile and click on the Released button to change the Global policy configuration mode to Released. Acknowledge the Warning message as required. You must release each CPE Test-Head test profile separately.

10 Distribute the CPE Test-Head profile locally to the managed OS 6250M devices.

Note — Policies are also automatically distributed to devices when the policies are used by resources on the device. See chapter 46 for more information about policies and policy distribution.

i Choose the CPE Test-Head profile and click on the Distribute button. The Distribute - CPE Test Head Profile form opens.

ii Choose the appropriate nodes from the Available Nodes column and click on the Move-right button.

iii Click on the Distribute button and close the form.

11 Configure the VLAN and port settings for the CPE Test-Head profile.

i Choose the CPE Test-Head profile and click on the Properties button to view the profile parameter settings.

ii Click on the Local Definitions tab button and click on the Search button. The OS 6250 devices to which the test policy was distributed in step 10 appears.

iii Choose an OS 6250M device from the list and click on the Properties button. The CPE Test-Head Profile form opens with the General tab displayed.

iv In the VLAN panel, click on the Select button for the Service ID parameter. The Select vlanSitePointer - CPE Test-Head Profile form opens.

v Click on the Search button to list the VLAN sites.

vi Choose a device and click on the OK button.

vii Click on the Local Audit On button to change the mode to Local Edit only.

viii Click on the Select button for the Port parameter. The Select vlan port - CPE Test-Head Profile form opens.

ix Click on the Search button to list the ports.

x Choose a port and click on the OK button.

xi Click on the Apply button and close the form.

12 As required, repeat steps 1 to 11 if you need to create additional CPE SLA Test-Head profiles. You can group profiles as described in step 13, otherwise, go to step 15.

Create a CPE SLA Test-Head Group profile

13 If required, create a CPE SLA Test-Head Group profile which can be use to bind individual CPE Test-Head profiles to form a group of tests.

i Choose Tools→AOS CPE Test-Head Profiles→CPE Test-Head Group Profile from the 5620 SAM main menu. The CPE Test-Head Group Profile form opens.

ii Click on the Create button. The CPE Test-Head Group Profile, Global Policy (Create) form opens.

iii Configure the following parameters:

- Name
- Description
- Source Endpoint
- Destination Endpoint
- Direction
- Role
- Tx Rate (kbps)

Note — If the Role parameter is set to the Generator option, perform step 14 otherwise, continue with step 13.

iv Click on the CPE Test Group Member tab button and click on the Create button. The Select Port - CPE Test Group Profile - Global Policy forms opens.

v Choose the appropriate CPE Test-Head profiles from the list and click on the OK button. The CPE Test-Head Group Profile, Global Policy (Create) form opens displaying the selected profiles.

vi Click on the OK button to save CPE Test-Head Group profile.

vii Click on the Search button to display the CPE Test-Head Group profile.

viii Choose the CPE Test-Head Group profile and perform steps 9, 10, and 11.

ix Go to step 15.

14 Configure the required feeder port for the generator.

i On the 5620 SAM network topology map, right-click on the appropriate OS 6250M device, and choose Properties from the contextual menu. The Network Element - <*Node Name*> (Edit) form appears.

ii Click on the Globals tab button.

iii Click on the AOS OAM tab button.

iv Click on the Select button that is associated with the Feeder Port Name parameter. The Select Feeder Port - Network Element - <*Node Name*> form appears.

v Click on the Search button to list the feeder ports.

vi Choose the appropriate feeder port and click on the OK button. The Network Element - <*Node Name*> (Edit) form reappears.

vii Click on the OK button to save the feeder port information.

viii Perform the rest of the substeps in step 13.

Configure the STM test execution details

15 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

16 Click on the Create button and choose one of the following options:

a AOS CPE→CPE SLA Test—Allows you to run a test on a CPE test-head profile or a group of profiles. The CPE SLA Test, CPETest-0 (Create) form opens with the General tab displayed. Perform steps 17 to 20, and step 22 to configure this option.

b AOS CPE→CPE SLA Test Group—Allows you to run several tests on a on a CPE test-head profile or group of profiles. The CPE SLA Test Group, CPETest-0 (Create) form opens with the General tab displayed. Complete steps 17, 18, 20, 21, and step 22 to configure this option.

17 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

18 In the Generator panel, click on the Select button. The Select Generator - CPE SLA Test - CPET Test-0 form opens.

i Click on the Search button to list the generator profiles.

ii Choose a generator profile and click on the OK button to close the form.

19 In the Analyzer panel, click on the Select button. The Select Analyzer - CPE SLA Test - CPET Test-0 form opens.

i Click on the Search button to list the analyzer profiles.

ii Choose an analyzer profile and click on the OK button to close the form.

20 Click on the Test Parameters tab button and configure the following parameters:

- Number of Test Iterations
- Test Iteration Duration
- Generator Tx Rate
- Generator Frame Size (bytes)
- Increase Tx Rate Every Iteration

21 Click on the CPE SLA Test Group Members tab button and click on the Create button. The CPE Test-Head Group Profile - CPE SLA Test Group CPETestGroup - 0 forms opens.

i Click on the Search button to display the CPE Test-Head Group profiles.

ii Choose the appropriate CPE Test-Head Group profiles and click on the OK button to close the form. The CPE SLA Test Group, CPETest-0 (Create) form reappears.

22 Click on the OK button to close the form.

Run the STM test and analyze the results

23 In the Service Test Manager (STM) form, choose one of the following options from the Test (Assurance) drop-down menu and click on the Search button.

a CPE SLA Test (AOS SAS)—This option displays all single CPE test-head profile tests that have been created.

b CPE SLA Test Group (AOS SAS)—This option displays all group CPE test-head profile tests that have been created.

24 Choose the appropriate CPE SLA test and click on the Execute button to start the test.

25 To view the test results, click on the Results tab.

78.10 Workflow to use the Service Test Manager

1 If you are configuring an OAM or an Ethernet CFM test, review the appropriate workflow.

a Review "Workflow to use OAM diagnostic tests" in chapter 38.

b Review "Workflow to configure Ethernet CFM" in chapter 78.

2 As required, configure the STM default settings to meet your operational requirements:

a Configure OAM test IDs if your 5620 SAM system is a redundant deployment. See Procedure 78-1 for more information.

b Modify the STM default system preferences. See Procedure 78-2 for more information.

c Enable the debug STM mode, which allows you to access more options on the STM form. See Procedure 78-3 for more information.

3 Create or modify an STM test policy to define the generated tests for the STM test suite. See Procedure 78-4 or 78-5 for more information.

4 As required, configure the threshold-crossing alarms for test policies, test definitions, and assurance tests.

a Configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy. See Procedure 78-6 for more information.

b Configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy. See Procedure 78-7 for more information.

5 Create or modify an STM test suite. See Procedure 78-8 or 78-9 for more information.

- Choose the type of entity to which the suite applies.
    - Choose None if you want to include tests that are associated with different types of entities, such as VLL and Tunnel (SDP).
- As required, associate a test policy with the test suite
- As required, choose tests for the first-run test group.
- As required, generate tests for the test suite.
- As required, choose tests for the last-run test group.

6 As required, create a schedule for an STM test suite that you want to execute regularly for continual network monitoring. To schedule the execution of a test suite, you must first create the SAM schedule. See chapter 79 for information about creating schedules.

a Schedule the execution of a test suite using a SAM schedule. See Procedure 78-10 for more information.

b Configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy. See Procedure 78-11 for more information.

c As required, modify the default size constraint policy or create additional size constraint policies to control the database resource usage by scheduled STM tasks. The default size constraint policy limits the number of STM results to 50 000 to avoid system performance degradation. See chapter 46 for more information about creating size constraint policies to limit the space consumed by historical records in the 5620 SAM database.

d Enable the scheduled tasks.

e Apply schedules to test suites as required to create scheduled tasks.

7 Execute the STM test suite. See Procedure 78-12 more information.

8 Monitor the diagnostic results from the scheduled test suites and the alarm list for indications of network or service faults and threshold-crossing alarms.

a View aggregated test suite results. See Procedure 78-13 for more information.

b View and compare test suite results for a tested entity. See Procedure 78-14 for more information.

c View and compare test suite results. See Procedure 78-15 for more information.

78.11 Service Test Manager procedures

The following procedures describe how to perform 5620 SAM STM tasks.

Procedure 78-1 To configure OAM test IDs

Note — If the 5620 SAM system is a redundant deployment, you must perform this procedure on each 5620 SAM main server in the cluster.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Open the nms-server.xml file with a plain-text editor.

4 Locate the following tag that marks the beginning of the ID manager section:

```
<idManager>
```

5 Add the following before the end of the ID manager section:

```
<range name="testId" min="xx" max="yy"/>
```

where
xx is the minimum value for the test ID range; for example, 10000
yy is the maximum value for the test ID range; for example, 50000

Note 1 — The test ID ranges for the 5620 SAM servers must not overlap.

Note 2 — The primary and standby 5620 SAM servers must use the same test ID range.

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the console prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM server reads the nms-server.xml file and puts the configuration change into effect.

10 Close the console window.

Procedure 78-2 To modify the STM default system preferences

1 Choose Administration→System Preferences from the 5620 SAM main menu. The System Preferences form opens.

2 Click on the Test Manager tab button.

3 As required, configure the following parameters:

   a Maximum Number of Results in Database

   b Default Test Result Storage

   c Log Retention Time (minutes)

   d Log Rollover Time (minutes)

4 Click on the OK button. A confirmation dialog box is displayed.

5 Click on Yes. The System Preferences form closes.

Procedure 78-3 To enable the debug STM mode

Perform this procedure to enable debug STM mode, which allows you to access more options from the Service Test Manager (STM) form.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Debug STM Mode parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 78-4 To create a STM test policy

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NE Schedulable
- Entity Type
- Strategy
- Lightweight Execution
- Ignore Probe Results
- Accounting Files
- Continuously Executed
- Test Result Storage

The Strategy parameter is only configurable when the Entity Type parameter is set to VLL Services.

The Lightweight Execution, Ignore Probe Results, Accounting Files, Continuously Executed, and Test Result Storage parameters are configurable when the NE Schedulable parameter is enabled.

The Continuously Executed and Test Result Storage parameters are only configurable when the Accounting Files parameter is enabled.

Note 1 — You must enable the NE Schedulable parameter if the test suite that you create using the policy is to become an NE scheduled task.

Note 2 — If you are creating a CFM Ethernet test, you must enable the NE Schedulable parameter, and optionally you can configure the Accounting Files and Continuously Executed parameters. You must select VLL Service, VPLS, or Composite Service for the Entity Type parameter.

5 Click on the Test Definitions tab button.

6 Click on the Add button to add a test definition to the test policy. A cascading submenu appears.

7 Choose an option from one of the categories in the cascading submenu. The options vary, depending on the Entity Type and NE Schedulable parameter values you specified in step 4. For example, Ethernet CFM test definition options only appears if you selected either the VLL Service or VPLS option as the Entity Type and if you also enabled the NE Schedulable parameter.

Each option in this step has three tabs that contain configurable parameters: General, Test Parameters, and Results Configuration. Parameters that are common to all options are listed in the remainder of this step. Parameters that are specific to a particular option will be configured in step 8.

The following configurable parameters appear on the General tab of the configuration form for every option:

- Name
- NE Persistent
- Description
- NM Administrative State

The NE Persistent parameter is configurable only if you did not enable the NE Schedulable parameter in step 4.

The following configurable parameters appear on the Test Parameters tab of the configuration form for most options in this step:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

A combination of the following configurable parameters appears on the Results Configuration tab of the configuration form for most options in this step:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Maximum Failures
- Trap Generation

8 Perform this step to configure the parameters that are specific to the particular test definition you are creating.

Choose the required test definition option from the following:

a Site ping test definition (Service→Add Site Ping) for a VLL service, VPLS, VPRN service, mirror service, service connector, or router:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Use Local Tunnel
- Use Remote Tunnel

iii Go to step 9.

b VCCV ping test definition (Service→Add VCCV Ping) for a VLL service:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Go to step 9.

c VCCV trace test definition (Service→Add VCCV Trace) for a VLL service:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Go to step 9.

d MAC ping test definition (Service→Add MAC Ping) for a VLL service or VPLS:

i Configure the following parameters on the General tab:

- Target MAC Address
- Source MAC Address

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

iv Go to step 9.

e MEF MAC ping test definition (L2 Service→Add MEF MAC Ping) for a VPLS:

Note — This test is only supported on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0 nodes.

i Configure the Target MAC Address parameter on the General tab.

ii Click on the Test Parameters tab button.

iii Configure the Size (octets) parameter.

iv Click on the Results Configuration tab button.

v Configure the Trap Generation parameter.

vi Go to step 9.

f Multicast FIB ping test definition (Multicast→Add MFIB Ping) for a VPLS:

i Configure the following additional parameters on the General tab:

- Multicast Source
- Multicast Group

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Time To Live
- Reply Via Control Plane

iv Go to step 9.

g Ping test definition (L3 Service→Add VPRN Ping) for a VPRN:

  i Click on the Test Parameters tab button.

  ii Configure the parameters:

  - Time To Live
  - Reply Via Control Plane

  iii Go to step 9.

h Trace test definition (L3 Service→Add VPRN Trace) for a VPRN:

  i Click on the Test Parameters tab button.

  ii Configure the parameters:

  - Initial Time to Live
  - Maximum Time to Live
  - DiffServ Field
  - Reply Via Control Plane

  iii Go to step 9.

i Multicast routing information test definition (Multicast→Add mrinfo) for a VPRN or router:

  i There are no parameters that are specific to the mrinfo test definition.

  ii Go to step 9.

j Multicast trace test definition (Multicast→Add mtrace) for a VPRN or router:

  i Click on the Select button on the General tab to choose a multicast group to run the trace against.

  ii Click on the Test Parameters tab button.

  iii Configure the parameters:

  - Initial Time to Live
  - Maximum Number of Hops

  iv Go to step 9.

k ICMP ping test definition (ICMP→Add ICMP Ping) for a VPRN or router:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

iii Go to step 9.

l ICMP trace test definition (ICMP→Add ICMP Trace) for a VPRN or router:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- DiffServ Field
- Time To Wait (milliseconds)

iii Go to step 9.

m Tunnel ping test definition (Service Transport→Add Tunnel Ping) for a service tunnel:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile

iii Go to step 9.

n MTU ping test definition (Service Transport→Add MTU Ping) for a service tunnel:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)

iii Go to step 9.

o Ping test definition (MPLS→Add LSP Ping) for an LSP:

i In the General tab, configure the Target Type parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Go to step 9.

p Trace test definition (MPLS→Add LSP Trace) for an LSP:

i In the General tab, configure the Target Type parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iv Go to step 9.

q Ping test definition (MPLS→Add P2MP LSP Ping) for a P2MP LSP:

i In the General tab, configure the Select All S2L Paths parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Go to step 9.

r Trace test definition (MPLS→Add P2MP LSP Trace) for a P2MP LSP:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iii Go to step 9.

s Ping test definition (L1/L2→Add ATM Ping) for an ATM PVC:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Loopback Location (hex)
- Destination Type

iii Go to step 9.

t CFM loopback test definition (Ethernet CFM→Add CFM Loopback) for a VLL service or VPLS:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)

iii Go to step 9.

u CFM link trace test definition (Ethernet CFM→Add CFM Link Trace) for a VLL service or VPLS:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- TTL

iii Go to step 9.

v CFM two way delay test definition (Ethernet CFM→Add CFM Two Way Delay Test) for a VLL service or VPLS:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile

iii Go to step 9.

w CFM two way SLM test definition (Ethernet CFM→Add CFM Two Way SLM) for a VLL service or VPLS:

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Class
- Forwarding Profile
- Size (octets)

iii Go to step 9.

9 To configure threshold-crossing alarms as required, perform the following:

a Click on the Thresholds tab.

b Perform steps 9 to 15 of Procedure 78-7.

10 Click on the OK button. The Definition Create form closes and a dialog box appears.

11 Click on the OK button. The Test Policy (Create) form reappears with the new OAM test definition listed.

12 Perform steps 5 to 11 to add additional OAM test definitions to the policy.

13 If you added Ethernet CFM test definitions to the test policy then go to step 14. Otherwise go to step 18.

14 Click on the CFM Details tab.

15 Click the Select button to choose a MD Mgr Object ID. The Select Maintenance Domain form is displayed.

16 Click the Search button and choose the required maintenance domain from the list.

17 Click OK. The Select Maintenance Domain form closes and the selected MD Mgr Object ID is displayed in the CFM Details tab.

18 Click on the OK button. The Test Policy (Create) form closes.

19 Close the Service Test Manager form.

Procedure 78-5 To modify a test policy

Note — If you modify a test policy associated with a test suite, you must regenerate the Generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies appears.

5 Select a test policy and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Configure the Name and Description parameters, as required.

7 Click on the Test Definitions tab button.

8 Perform one of the following:

- **a** Select a test definition in the list and click on the Properties button.
- **b** Click on the Add button to add a test definition to the test policy.

9 Click on the OK button to return to the Policy form.

10 Modify the parameters for the test definition, as required.

11 Click on the Update Test Suites button to apply the test policy changes to all test suites that are associated with the test policy.

Caution — The operation of scheduled test suites that use the test policy may be adversely affected if you modify the test policy while a scheduled task for the suite is enabled.

12 Click on the Usages tab button to view a list of the test suites that use the test policy.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button to confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

15 Click on the Close button to close the Service Test Manager form.

Procedure 78-6 To configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy

Perform this procedure to configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is NE-schedulable applies just to the test.

Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies is displayed.

5 Choose an NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Click on the Test Definitions tab. A list of tests associated with the policy opens.

7 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

8 Click on the Thresholds tab.

9 Click on the Add button. The Threshold Event Definition (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

11 Click on the Rising Threshold tab.

12 Configure the Threshold Value parameter.

13 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition (Create) form.

14 Configure the Threshold Value parameter.

15 Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.

16 Click on the OK button. The test appears on the list.

17 Repeat steps 9 to 16 to configure threshold events on additional tests.

18 Click on the OK button. The Test Definition—Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

19 Click on the OK button. A dialog box appears.

20 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

21 Close the Service Test Manager form.

Procedure 78-7 To configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy

You can configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are non-NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Non-NE-schedulable OAM tests can be configured as NE persistent. NE persistent tests are deployed to the network node after the first execution and remain on the node each time the test is executed. The type of threshold-crossing event available for selection depends on the test type.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is non-NE-schedulable applies just to the test.

Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies is displayed.

5 Choose a non-NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Click on the Test Definitions tab. A list of tests associated with the policy opens.

7 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

8 Click on the Thresholds tab.

Note — The Thresholds tab is enabled or disabled depending on the test type selected in step 7. Threshold alarm events can not be configured for Site Ping, mrinfo, mtrace, VPRN Trace and Mtu Ping tests.

9 Click on the Create button. The Threshold Event Definition (Create) form opens with the General tab displayed.

10 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

11 Click on the Rising Threshold tab.

12 Configure the Threshold Value parameter.

13 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition, (Create) form.

14 Configure the Threshold Value parameter.

15 Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.

16 Click on the OK button. The test appears on the list.

17 Repeat steps 9 to 16 to configure threshold events on additional tests in the policy.

18 Click on the OK button. The Test Definition, Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

19 Click on the OK button. A dialog box appears.

20 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

21 Close the Service Test Manager form.

Procedure 78-8 To create a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Test Suite from the contextual menu. The Test Suite (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NE Schedulable
- Entity Type
- Validation Test Suite
- Timeout (minutes)
- First Run Execution Sequence
- Last Run Execution Sequence

Note 1 — The Entity Type parameter specifies that only test policies created for the same entity type are available for the test suite. The parameter also restricts the predefined tests that are available as first-run or last-run tests to those that apply to the entity type.

Note 2 — To create a test suite that includes tests for different entity types, specify None as the Entity Type parameter value. This allows you to choose any predefined test as a first-run or last-run test.

Note 3 — Specifying None as the Entity Type parameter value disables the generation of tests in a test suite; the policy that STM uses to generate tests must be associated with a specific entity type.

Note 4 — The Validation Test Suite parameter specifies that the test suite is used to validate the connectivity of the tested service entity to which it is applied. OAM validation tests are not supported for HVPLS.

Click on the More Actions button and choose Validate on the associated service or service tunnel configuration form to run the OAM validation test. The results of the OAM validation test are indicated by the OAM Validation Failed operational flag.

Note 5 — First Run and Last Run tests can be added for test suites that have the Continuously Executed and Accounting Files options enabled can be added to test suites.

Note 6 — When issuing an Execute or Stop command for a test suite that has the Continuously Executed and Accounting Files options enabled, the execution or stopping of the First Run and Last Run tests will be triggered.

Note 7 — If you are creating an Ethernet CFM test suite, you must enable the NE Schedulable parameter.

5 To create a scheduled task, see procedure 78-10.

6 If you chose None as the Entity Type parameter value in step 4, go to step 17. To create a scheduled task, go to step 7.

7 Click on the Test Policy tab button.

8 Click on the Add button to choose a test policy to associate with the test suite. The Select Test Policy - Test Suite form opens.

9 Click on the Search button to display a list of available test policies.

Note — Only test policies that apply to the type of entity specified by the Entity Type parameter in step 4 appear in the list.

10 Choose a test policy from the list and click on the OK button. The test policy appears on the Test Policy tab.

11 Click on the Tested Entities tab button.

12 Click on the Add button to choose a service, transport element, or device as the object against which the test suite is run. The Add form opens.

13 Click on the Search button to display a list of available entities.

Note — Only entities that match the type of entity specified in the test policy appear in the list.

14 Choose an entity from the list and click on the OK button. The Add form closes and an entry for the entity appears in the list on the Tested Entities tab.

15 Ensure the item is selected in the list and click on the Lock Test Generation button, if required.

Note — Locking the test generation means that the initial settings you specify when creating the test suite will be retained, even if later on you change some attributes (for instance, if you are testing SDP tunnels and you extend the tested entities by selecting another SDP tunnel). All customized test attributes are retained when re-generating the tests.

The 5620 SAM auto-locks tested entities when generated tests are either modified or deleted.

The Test Re-generation locked field in the list will display a checkmark to indicate that the lock is enabled and the button's name changes to Unlock Test Generation. If you do not want to lock the test, then click the Unlock Test Generation button. The Test Re-generation locked field in the list will not display a checkmark.

16 Repeat steps 12 to 14 for each additional entity that you want to specify.

17 Click on the First Run Tests tab button.

18 Click on the Add button to choose a predefined test that is to execute before the generated tests in the suite. The Add form opens.

19 Click on the Search button to display a list of available tests.

20 Choose a test from the list and click on the OK button. The Add form closes and the test entry appears on the First Run Tests tab.

21 Repeat steps 18 to 20 for each additional first-run test that you want to specify.

22 When there is more than one test in the first-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the first-run test execution sequence, if required.

23 Click on the Last Run Tests tab button.

24 Click on the Add button to include a predefined test that is to execute after the other tests in the suite have completed. The Add form opens.

25 Click on the Search button to display a list of available tests.

26 Choose a test from the list and click on the OK button. The Add form closes and the test entry appears on the Last Run Tests tab.

27 Repeat steps 24 to 26 for each additional last-run test that you want to specify.

28 When there is more than one test in the last-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the last-run test execution sequence, if required.

29 Click on the Apply button to save the changes. Additional buttons at the bottom of the form become active.

30 If you chose None as the Entity Type parameter value in step 4, go to step 34.

31 Click on the Generated Tests tab button.

32 Click on the Generate Tests button. The 5620 SAM begins generating tests for the test suite based on the test policy. The tests appear in a list on the Generated Tests form as they are generated.

Note 1 — When the test policy or the configuration of an entity on the Tested Entities tab changes, you must regenerate the tests in the test suite by clicking on the Generate Tests button.

Note 2 — When tests have been generated in a Test Suite (which has a test policy already associated to it), these existing tests will not be altered (delete and recreated, or set to default tests), when the Generate Tests button is pressed again.

33 Click on the Generation Logs tab button to view the log file that the 5620 SAM creates during test generation, as required.

Note — Generation Logs messages only appear if any failures occur during the test generation process.

34 Click on the OK button to close the Test Suite (Create) form.

35 Close the Service Test Manager form.

Procedure 78-9 To modify a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Select a test suite and click on the Properties button. The Test Suite (Edit) form opens with the General tab displayed. Use the parameters on this tab to change the execution order of tests in the First run and Last run test groups, as required.

The following tabs list the test-suite components that you can individually or collectively add to or remove from the test suite:

- Test Policy tab — displays the test policy that is associated with the test suite
- Tested Entities tab — lists the entities that are objects of the tests in the test suite
- First Run Tests tab — lists the group of tests in the test suite that run first
- Generated Tests tab — lists the generated tests that are included in the test suite
- Last Run Tests tab — lists the group of tests in the test suite that run last

The following tabs display information about the creation and execution of the test suite:

- Results tab — lists the historical results that are returned by each execution of the test suite
- Generation Logs tab — lists the log entries that are created during test generation for the test suite
- Faults tab — displays the faults associated with the test suite

Note — Generation Logs messages only appear if any failures occur during the test generation process.

6 Modify the parameters for the test suite, as required.

To configure an item on a tab that contains a list of test-suite components, select the item and click on the Properties button.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Test Suite (Edit) form closes and the Service Test Manager form reappears.

9 Click on the Close button to close the Service Test Manager form.

Procedure 78-10 To schedule the execution of a test suite using a SAM schedule

To schedule the execution of a test suite using a SAM schedule, you must first create the SAM schedule. See chapter 79 for information about creating schedules.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Double-click on the test suite that you want to schedule. The Test Suite (Edit) form opens with the General tab displayed.

6 Click on the Schedule button. The SAM Scheduled Task (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

Caution — Setting the Administrative State parameter to Enabled puts the scheduled task into effect according to the schedule parameters. Ensure that the test suite and the objects to which it applies are appropriately configured before you set the parameter to Enabled.

8 Click on the Select button. The Select Schedule - SAM Scheduled Task form opens.

9 Select a schedule and click on the OK button. The chosen schedule appears on the form.

10 Click on the OK button. The SAM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

11 Close the Test Suite (Edit) form.

12 Close the Service Test Manager form.

Procedure 78-11 To schedule the execution of a test suite using an existing NE schedule

To schedule the execution of a test suite using an existing NE schedule, perform Procedure 79-6 to turn up the NE scheduled task.

Procedure 78-12 To execute a STM test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Select a test suite in the list and click on the Properties button. The Test Suite (edit) form opens with the General tab displayed.

6 Click on the Execute button. Execution of the test suite begins and the Test Suite (edit) form displays the Results tab. You can view the test results when the test execution is complete.

Note — You can run an OAM validation test from the Properties form of a service tunnel or an applicable service. See the applicable service management chapter for more information.

7 Close the Test Suite (edit) form.

Procedure 78-13 To view aggregated test suite results

Perform this procedure to view test suite results from the Test Suite Result (Edit) form.

Note 1 — You can also view the test suite results for an object from the Tests tab of the configuration form for the object.

Note 2 — You can reorder a column in a tabular information view by dragging the column heading to the desired position, then right-clicking on the column heading and choosing Save Table Preferences.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

3 Click on the Aggregated Result (Assurance) icon below the Result (Assurance) icon to expand the selection.

4 Choose one of the following objects in the tree display below Aggregated Result (Assurance).

   a Select Test Definition Result (Assurance) to create a search filter based on a test definition.

   b Select Test Policy Result (Assurance) to create a search filter based on a test policy.

   c Select Test Suite Result (Assurance) to create a search filter based on a test suite.

5 Configure the filter criteria.

Caution — Ensure that the filter properties chosen are sufficient to appropriately limit the number of returned result entries. Otherwise, the number of returned entries may exceed the maximum number that the 5620 SAM permits, and valid entries may not appear in the list.

6 Click on the Search button. A list of test suite results appears.

7 Select a test suite result and click on the Properties button. The Test Suite Result (Edit) form opens with the General tab displayed.

8 View the general results on the General tab.

Note — If the test suite uses a test policy with the Lightweight Execution parameter enabled, only the General and Failed Test tabs are available.

9 Click on the First Run Results tab button to view test results from individual tests in the first-run test group of the test suite.

10 Click on the Summary By Policy tab button to view test results for individual tests in the test suite, listed by test policy.

11 Click on the Summary By Definition tab button to view test results for individual tests in the test suite, listed by test definition.

12 Click on the Last Run Results tab button to view test results from individual tests in the last-run test group of the test suite.

13 Close the Test Suite Result (Edit) form.

14 Click on the Close button to close the Service Test Manager form.

Procedure 78-14 To view and compare test suite results for a tested entity

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down menu.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Choose a test suite in the list and click on the Properties button. The Test Suite (edit) form opens with the General tab displayed.

6 Click on the Tested Entities tab button to view a list of entities tested by the test suite.

7 Choose a tested entity from the list and click on the Show Results button. The Tested Entity Result (edit) form opens.

8 Configure the filter criteria.

9 Click on the Search button. A list of test results appears.

10 Choose a test result from the list and click on the Properties button. The result form for the selected test opens.

11 Close the result form.

12 If you need to compare the results of two tests of the same type, choose two results for the test from the displayed list and click on the Compare button; the Difference form opens. Otherwise, go to step 15.

13 Compare the results of the test results.

14 Close the Difference form.

15 Close the Tested Entity Result (edit) form.

16 Close the Test Suite (Edit) form.

17 Close the Service Test Manager (STM) form.

Procedure 78-15 To view and compare test suite results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test results appears.

5 Choose a test result and click on the Properties button to view the properties of the test. The selected test type result (Edit) form opens.

6 If you need to compare the results of two tests within a test suite, choose two test results of the same type within a test suite and click on the Compare button; the Difference form opens. You can view the test values for each test. Otherwise, go to step 8.

7 Close the Difference form.

8 Close the test type result (Edit) form.

9 Close the Service Test Manager (STM) form.

Procedure 78-16 To delete a test suite

1 If the test suite is scheduled, you must remove the scheduled task associated with the test suite before you can delete the test suite. See chapter 79 for more information.

2 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

3 Choose Test Suite (Assurance) from the object drop-down list.

4 Configure the filter criteria.

5 Click on the Search button. A list of test suites appears.

6 Select a test suite in the list and click on the Delete button. A dialog box appears.

7 Click on the Yes button to confirm the action. The test suite is deleted and removed from the list.

8 Click on the Close button to close the Service Test Manager form.

79 — Scheduling

79.1 Scheduling overview

The 5620 SAM scheduling functions allow the creation of 5620 SAM-based schedules for the automatic execution of tasks at designated times.

You can associate a schedule that you create using the 5620 SAM with a task that supports scheduling. A task such as running an STM test suite can be immediately processed, scheduled for later execution, or retained for future use. A task that is associated with a schedule is called a scheduled task. A scheduled task must be created in the configuration form for the task. For example a STM test suite scheduled task must be created in the STM test suite configuration form. After scheduled tasks are created they are associated with a schedule.

A 5620 SAM schedule is configurable for one-time or ongoing task execution. You can optionally specify the time at which an ongoing schedule is to stop functioning.

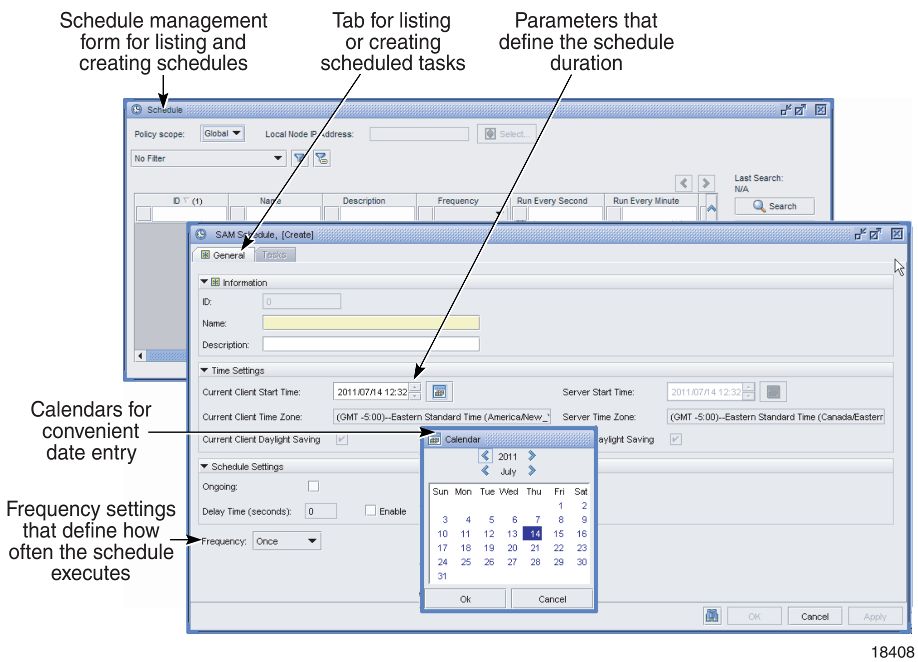
To simplify creating 5620 SAM-based schedules when the user and server are in different time zones, the 5620 SAM converts and displays schedule times specific to the user and server. For example, if a user in Ottawa wants to schedule a task on a 5620 SAM server in London, the 5620 SAM calculates the time difference and displays the user and server local times.

User time zones are configured in the user preferences form. If a time zone is not configured on the main server, the 5620 SAM uses the default time zone on the single-user client or client delegate server station, If the default time zone is not one of the 5620 SAM time zone options, the 5620 SAM displays the time zone ID and uses the UTC value without the time zone offset.

The 5620 SAM displays whether daylight saving time is in effect for the client and the server. Daylight saving time is specified for the user start time and is based on the client time zone. Daylight saving time does not specify the current time and end time.

Figure 79-1 shows the Schedule management form and the SAM Schedule configuration form.

Figure 79-1 Schedule management and configuration forms



SAM schedules

A SAM schedule exists only in the 5620 SAM and is not deployed to the target NEs. When a configured SAM schedule run time arrives, the 5620 SAM executes the associated task and compiles the task results for presentation to 5620 SAM clients.

A delay time for executing SAM scheduled runs can be configured to delay the execution of a run within a scheduled task in cases when a previously scheduled run is still executing. The 5620 SAM attempts to execute the new run at the configured delay time; if the run cannot execute at the delay time, the 5620 SAM skips the scheduled run. When a previous run completes and the next scheduled run is triggered, the run executes and is not delayed, whether a delay time is configured.

The SAM schedule functionality in the 5620 SAM uses the 5620 SAM server time zone to trigger the scheduled tasks.

A 5620 SAM-based schedule supports the following tasks:

- STM test suites. See chapter 78 for more information about STM test suites.
- NE software upgrades. See chapter 23 for more information about NE software upgrades.

Consider the following when you create a SAM schedule or a scheduled task.

- Ensure that scheduled tasks are run sufficiently far apart to allow one task to finish before the next starts. Otherwise, the next occurrence of the task is skipped or delayed, if the delay time is configured.
- Do not create schedules that overlap, as no validation is performed to ensure that a newly configured schedule does not overlap with an existing schedule.

- A new SAM scheduled task is shut down by default and must be turned up before it can be executed with one exception. Scheduled software upgrade tasks associated with all NE types are by default auto-enabled.
- Users with write access permissions to a specific schedule package can view or delete all the created schedules and scheduled tasks related to the package. Other users can only view schedules. See chapter 9 for more information about user permissions.
- By default, the 5620 SAM associates a scheduled task with the user account that is used to create the scheduled task. You can assign a different user account to a scheduled task. The user account must have the assigned scope of command role that is appropriate for the task, or the 5620 SAM does not execute the scheduled task.
- When you create a scheduled task that runs on a weekly or monthly schedule, you must reset the scheduled task when daylight savings time is in effect. See Procedure 79-9 for information about resetting schedules.
- If a schedule is not synchronized with the server time, you must reset the scheduled task. See Procedure 79-9 for information about resetting schedules
- SAM schedules are not distributed to the target NEs.
- You cannot delete a schedule that has a dependency, for example, one that is associated with a task.
- One minute is added to the default start and end time values of a 5620 SAM-based schedule to allow time for schedule configuration.
- A monthly SAM schedule with the Run Every Month or Run Every Months parameter configured uses a 30-day interval.
- When you create a monthly SAM schedule using the Run Every parameter and specify a date that does not exist for the specified months, the last date of the month is used. For example, if you create a monthly scheduled task, starting January 31st, the scheduled task will run on February 28th, March 31st and April 30th when those months are specified in the schedule.

79.2 Workflow to manage scheduling

1. Create a task, such as an STM test suite, that supports the 5620 SAM scheduling function.
2. Create or modify a SAM schedule. See Procedure 79-1 or 79-2 for more information.
3. Associate a task with the schedule. See Procedure 79-3 or 79-4 for more information.
4. For a SAM scheduled task that requires user account privileges other than the default privileges, assign a different user account to the scheduled task. See Procedure 79-5 for more information.
5. Turn up the scheduled task. See Procedure 79-6 for more information.

6 After the schedule executes the task, review the current status of the SAM scheduled task. See Procedure 79-7 for more information.

7 As required, perform one of the following.

a execute the scheduled task immediately; see Procedure 79-8 for more information

b reset the scheduled task; see Procedure 79-9 for more information

c delete the scheduled task; see Procedure 79-10 for more information

d delete the schedule; see Procedure 79-11 for more information

79.3 Scheduling procedures

Use the following procedures to manage 5620 SAM schedules and scheduled tasks.

Procedure 79-1 To create a SAM schedule

1 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

2 Click on the Create button. A SAM Schedule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Current Client End Time
- Current Client End Time
- Current Client Start Time
- Current Client End Time
- Ongoing
- Delay Time (seconds)
- Enable
- Frequency

The Current Client End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the Current Client End Time expires.

4 Perform one of the following that corresponds to the Frequency parameter value that is specified in step 3:

a When the parameter is set to Once, go to step 5.

b When the parameter is set to Per Second, configure the following parameters:

- Run Every Second
- Run Every Seconds

c When the parameter is set to Per Minute, configure the following parameters:

- Run Every Minute
- Run Every Minutes

d When the parameter is set to Per Hour, configure the following parameters:

- Run Every Hour
- Run Every Hours

e When the parameter is set to Per Day, configure the following parameters:

- Run Every Day
- Run Every Days
- Run Every

f When the parameter is set to Per Week, configure the following parameters:

- Run Every Week
- Run Every Weeks
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

g When the parameter is set to Per Month, configure the following parameters:

- Run Every Month
- Run Every Months
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

5 Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Schedule form reappears.

6 Close the Schedule form.

Procedure 79-2 To modify a schedule

Perform this procedure to change the configuration of a schedule. You cannot modify a schedule that is in use by a scheduled task.

Note — You can modify a schedule only when you are logged in as the user that is assigned to the schedule. To assign a different user account to the schedule, perform Procedure 79-5.

1. Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.
2. Choose SAM Schedule from the object drop-down list.
3. Configure the filter criteria. A list of schedules is displayed.
4. Select an entry in the list and click on the Properties button. The SAM Schedule (Edit) form opens.
5. Modify the parameters, as required.
6. Click on the OK button. The SAM Schedule (Edit) form closes and the Schedule form reappears.
7. Close the Schedule form.

Procedure 79-3 To associate a task with a 5620 SAM schedule

1. Perform one of the following.
   - **a** Assign a SAM schedule to a task.
     - **i** Open the properties form for a task that supports SAM schedules, such as an STM test suite.
     - **ii** Click on the Schedule button. The *task_name* (Edit) form opens, go to step 2.
   - **b** View scheduled tasks associated with a SAM schedule.
     - **i** Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.
     - **ii** Choose SAM Schedule (Schedule) from the object drop-down list.
     - **iii** Configure the filter criteria. Click on the Search button. A list of SAM schedules is displayed.
     - **iv** Select a SAM schedule in the list and click on the Properties button. The SAM Schedule (Edit) form opens.

v Click on the Tasks tab button. A list of scheduled tasks appears.

vi Choose a task from the list. Click on the Properties button to view the scheduled tasks.

2 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

Note — When you set the Administrative State parameter to Enabled, the scheduled task goes into effect, according to the schedule parameters. Ensure that the task is appropriately configured before you set the parameter to Enabled.

3 Click on the Select button to choose a schedule. The Select Schedule - STM Scheduled Task *task_name* form opens with a list of schedules.

Note — The form lists only the schedules that are associated with the current 5620 SAM user.

4 Select a schedule in the list and click on the OK button. The Select Schedule - STM Scheduled Task *task_name* form closes and the scheduled task is displayed on the STM Scheduled Task (Create) form.

5 Click on the OK button. The STM Scheduled Task (Create) form closes.

6 Close the SAM Schedule (Edit) or task properties form.

7 Close the Schedule form if the form is open.

Procedure 79-4 To modify a scheduled task

Note — You can modify a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 79-5.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list and click on the Properties button. The scheduled task (Edit) form opens.

5 Modify the parameters, as required.

6 Click on the OK button. The SAM Scheduled Task (Edit) form closes and the Scheduled Task form reappears.

7 Close the Scheduled Task form.

Procedure 79-5 To assign a different user account to a SAM scheduled task

Perform this procedure to associate a SAM scheduled task with a different user account. By default, the 5620 SAM associates a scheduled task with the user account that is active when the SAM scheduled task is created.

> **Note —** The 5620 SAM does not execute a SAM scheduled task unless the scheduled task is associated with an existing 5620 SAM user account. If you delete the user account that is associated with a SAM scheduled task, you must assign a different user account to the SAM scheduled task. A 5620 SAM user with an assigned administrator scope of command role can assign a user account to a SAM scheduled task.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task list form opens.

2 Choose SAM Scheduled Task (schedule) from the object drop-down list.

3 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

4 Select a scheduled task and click on the Reassign User button. A dialog box informs you that the new user must have the appropriate access permissions to manage the scheduled task. See “Scope of command” in section 9.1 for more information.

5 Set the Change Current User To parameter.

6 Click on the OK button.

Procedure 79-6 To turn up or shut down a scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task (Schedule) from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select an entry in the list and click on the Task Action button.

5 Choose one of the following from the menu that appears:

   a Turn Up—enable the scheduled task. The administrative state changes to enabled.

   b Shut Down—disable the scheduled task. The administrative state changes to disabled.

6 Close the Scheduled Task form.

Procedure 79-7 To view the current status of a SAM scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

4 Select a SAM scheduled task in the list.

5 Click on the Task Action button and choose View Result from the menu that appears.

6 View the Execution Status indicator. The value is one of the following:

- None
- In Progress
- Skip Requested
- Skipped
- Stop Requested
- Stopped
- Succeeded
- Failed
- Delay Requested
- Delayed
- Started

7 View the Status indicator. The value is one of the following:

- Running—The scheduled task is running.
- Not Running—The scheduled task is not running.
- Completed—The scheduled task execution completed successfully.

8 Close the Scheduled Task form.

Procedure 79-8 To execute a SAM scheduled task

1 Turn up the SAM scheduled task, as described in Procedure 79-6.

2 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

3 Choose SAM Scheduled Task from the object drop-down list.

4 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

5 Select an entry and click on the Task Action button.

6 Choose Execute from the menu that appears. The 5620 SAM executes the SAM scheduled task.

7 Close the Scheduled Task form.

8 Perform Procedure 79-7 to view the SAM scheduled task execution status, if required.

Procedure 79-9 To reset a scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria to list tasks that the administrative state is enabled, and click on the Search button. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Turn Up button is enabled.

6 Click on the Task Action button and choose Turn Up from the menu that appears. The Shut Down button is enabled.

7 Close the Scheduled Task form.

Procedure 79-10 To delete a scheduled task

Note — You can delete a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 79-5.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Delete button is enabled.

6 Click on the Delete button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the scheduled task.

8 Close the Scheduled Task form.

Procedure 79-11 To delete a schedule

Note 1 — You cannot remove a schedule that is associated with a scheduled task; you must first delete the scheduled task.

Note 2 — You can delete a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 79-5.

1 Perform Procedure 79-10 to delete the scheduled tasks associated with the schedule.

2 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

3 Choose SAM Scheduled from the object drop-down list.

4 Configure the filter criteria. A list of schedules is displayed.

5 Select a schedule in the list and click on the Delete button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM deletes the schedule.

7 Close the Schedule form.

80 — Ethernet CFM

80.1 Ethernet CFM overview

The 5620 SAM Ethernet Connectivity Fault Management, or Ethernet CFM, function is implemented based on the IEEE 802.1ag OAM standard. This standard describes protocols for detecting, isolating, and reporting connectivity faults in an Ethernet network. You can use Ethernet CFM for the following:

- path discovery
- fault detection
- fault isolation
- fault notification

The IEEE 802.1ag OAM standard partitions a network into eight hierarchical levels called maintenance domains, or MDs. An MD is a network, or part of a network, that is provisioned with a set of maintenance entity groups, or MEGs, which are groups of service sites.

Typically, a MEG represents one service and consists of a group of maintenance end points, or MEPs. Only one MEG can be associated with a service, but one service can be associated with multiple MEGs. MDs and MEGs are distributed to NEs using the 5620 SAM policy distribution framework.

Within a MEG, MEPs can be divided into logical groupings called MEG sub-groups. MEG sub-groups allow you to group managed MEPs and unmanaged remote MEPs so that Ethernet CFM can be directed to a specific area of a system, a MEG sub-group, rather than the entire system.

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM continuity check
- CFM loopback
- CFM link trace
- CFM Eth test
- CFM two-way delay
- CFM one-way delay
- CFM single-ended loss (7705 SAR only)
- CFM two-way SLM

A CFM continuity check test is automatically generated when you create an MD. When you execute the test and a connectivity fault is present, the MEP that detects the fault raises an alarm. See Chapter 38 for information about a specific Ethernet CFM diagnostic test.

MEPs

MEPs are configured at the edge of an MD and perform the following functions:

- periodically send CFM continuity check messages
- validate CFM PDU replies
- discard CFM PDU messages that are not in the MEP configuration
- initiate and respond to CFM tests messages

MEPs can be added to services automatically or manually. The differentiator between these two options is the action results in associating a service with the MEG on all nodes versus associating a service with the MEG on a single node. See Procedure 80-1 for more information.

You can also add MEPs to services during Ethernet CFM test configuration from the Service Topology map. See “Working with Ethernet CFM objects” for more information.

Each MEP is assigned an up or down direction. An up MEP is provisioned on an ingress port, and monitors the forwarding path inside a bridge NE to the egress port. A down MEP is provisioned on an egress port, and monitors the forwarding path between bridge NEs. An up MEPs can be also provisioned on Virtual MEPs for B-VPLS, while a down MEP can be provisioned on facility MEPs

You can configure an initial MEP ID for automatic MEP ID assignment on an NE. See Procedure 80-2 for more information.

An up MEP can be associated with the following object types:

- Epipe and VPLS SAPs
- Epipe spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- VPLS and MVPLS B-sites, as virtual MEPs
- B-L2 access interfaces
- OmniSwitch VLAN SAPs

A down MEP can be associated with the following object types:

- Epipe, Ipipe, IES, VPLS, and VPRN SAPs
- Epipe and IES spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- B-L2 access interfaces
- MVPLS access interfaces
- OmniSwitch VLAN SAPs
- Network interfaces
- Ports
- LAGs

Virtual MEPs

A virtual MEP is an up MEP that is created on a B-VPLS or B-MVPLS site when a CFM continuity check test is run. Each virtual MEP transmits a CFM continuity check stream on all SAPs and SDPs of the site. A virtual MEP uses the site B-MAC address, if configured; otherwise, it uses the shelf MAC address. See chapter 71 for information about assigning virtual MEPs in B-VPLS and B-MVPLS.

The following rules apply to virtual MEP management:

- One virtual MEP can be configured on a VPLS or MVPLS B-site.
- All regular MEPs on SAPs and SDP bindings in the same MEG as a virtual MEP must be configured as up MEPs.

- Regular MEPs in the same MEG and on the same B-site as a virtual MEP cannot be enabled when the virtual MEP is enabled.
- Virtual MEPs can be created in a MEG only when MIP creation in the MEG is disabled.

Facility MEP

A facility MEP is a down MEP that is created on a network interface, port, or LAG. A facility MEP detects failure conditions for an Ethernet transport network using ETH-CCM or AIS and, where appropriate, propagates alarm conditions so that the services that share this common transport are aware of the failure.

A virtual facility Tunnel MEP is created by configuring a LAG MEP with a VLAN ID. In this instance the VLAN ID must match the outer encapsulation value of the SAP that is associated with the Tunnel MEP.

The following rules apply to facility MEP management:

- Only one facility MEP can be configured on a port, a LAG, or a network interface.
- A facility MEP can be configured on a port only if the MD level is 0.
- A facility MEP must be configured in the down direction.
- CCM is not supported if the MEP is configured on a network interface.
- Facility port MEPs are supported on ports in access or hybrid mode with Q in Q or dot1q encapsulation.
- Facility tunnel MEPs are supported on LAG ports configured with Q in Q encapsulation in access or hybrid mode.
- To configure MEPs on tunnels, the LAG VLAN ID must not be 0.
- Facility port MEPs cannot be configured on network elements that support Ethernet tunnels.
- The facility MEP ID must be unique within the same device.
- The facility tunnel MEP must have a lower MD level than any service MEPs that are created on the same LAG.

MIPs

Maintenance intermediate points, or MIPs, are internal points in an MD that perform the following functions:

- validate received CFM PDUs
- validate and respond to link trace messages
- validate and respond to loopback messages

A MIP consists of two half-function objects that allow the MIP to be recognized as a MIP in one MD level and as a MEP on a higher level.

Ethernet-CFM redundancy

When you configure Ethernet-CFM redundancy, you can link MEPs to the state of the resiliency mechanism that is supported in MC-LAGs. The state of the MEP does not affect the state of resiliency mechanism.

Ethernet-CFM redundancy is configured at the node level. When you configure Ethernet-CFM redundancy, the state of a MEP is the same as the state of the SAP, LAG, or MC-LAG with which it is associated. For example, if the redundant MC-LAG is in standby state, the MEP is also in standby state. When a MEP is in standby state, the MEP is idle, CCMs are not exchanged, and the MEP does not respond to CFM tests.

Note — The MEP, SAP, and LAG must reside within an MC-LAG that has Ethernet-CFM redundancy configured. See Procedure 43-1 to configure MC-LAGs.

When Ethernet-CFM redundancy is configured and the active state of an MC-LAG changes, the MC-LAG Inactive state on the MEP changes and any defects on the MEP are flagged.

The state of MEPs, SAPs, and LAGs that are configured for Ethernet-CFM redundancy appears in the MC-LAG Inactive field. The status of MC-LAGs that are configured for Ethernet-CFM redundancy appears in the Is Active field.

In addition to configuring Ethernet-CFM redundancy at the node level, you can configure Ethernet-CFM redundancy on tunnel MEPs. See Procedure 17-2 to configure Ethernet-CFM redundancy at the node level. See Procedure 18-14 to configure Ethernet-CFM redundancy on a tunnel MEP.

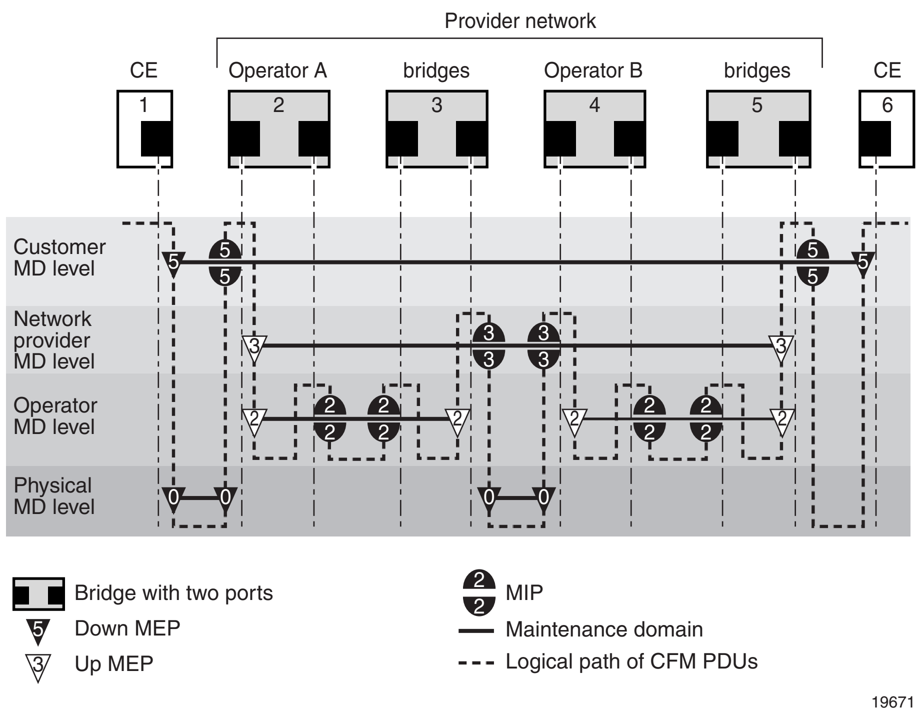
Sample Ethernet CFM implementation

Figure 80-1 shows an example of MDs, MEPs, and MIPs in a IEEE 802.1ag network that consists of two operator areas, for example, services in the provider network, that are joined to create a network path for customer traffic. The number on an object identifies the associated MD, which is one of the following:

- MD 5—end-to-end customer path
- MD 3—end-to-end network provider path
- MD 2—paths within services
- MD 0—physical path

MD 5 provides access to a down MEP on each CE device, and to a MIP on each PE bridge. MD 3 provides access to an up MEP on each PE bridge, and to a MIP on each bridge between groups of operator bridges. MD 2 provides access to the up MEPs and MIPs in each service. MD 0 provides access to MEPs for checking the physical connectivity between NEs.

Figure 80-1 Ethernet CFM objects in example network



Ethernet CFM implementation for composite services

End-to-end test suite generation for composite services is available for VPLS and VLL Epipe services. In this context, a composite service is a set of services connected by one or more of the following:

- Vlan uplinks
- Spoke bindings
- CCAG connectors

Creating test suites and test policies for composite services is very similar to creating these for a regular service. The Accounting Files and Continuously Executed options are also available when creating a test policy for a composite service.

Once tests have been ordered to generate, a MEG is created on each eligible endpoint SAP. Tests are then generated for this MEG that target all other eligible endpoint SAPs within the composite service. Results for individual tests can then be reviewed.

Note — If there is a previously-created MEG on one of the service sites (for example, perhaps one created for a service before it was included as a part of a composite service) and the Generate Tests button is selected, no tests will actually be generated. When a MEG with only a subset of the composite service already exists on one of the service SAPs, the generation of tests is blocked. That MEG must be first be deleted and the CFM tests can then be regenerated.

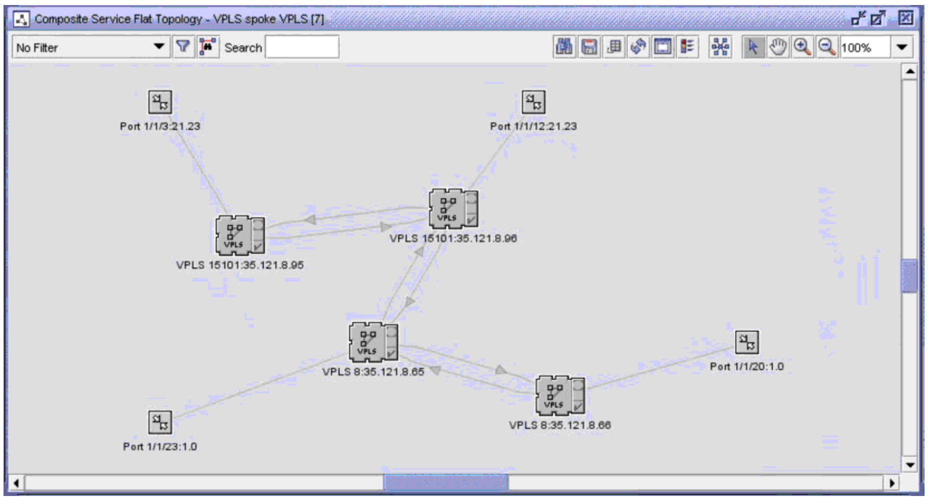
An overview and examples are provided to illustrate the steps and demonstrate the test generation rules and results for various configurations.

Examples of Ethernet CFM tests for composite services

The following examples illustrate how the Ethernet CFM test generation rules involving composite services are structured to operate.

The first is a simple configuration of two VPLSs (VPLS 8 and VPLS 15101) connected by a pair of spoke bindings between sites 35.121.8.96 and 35.121.8.65. It is shown in the flat topology view of Figure 80-2.

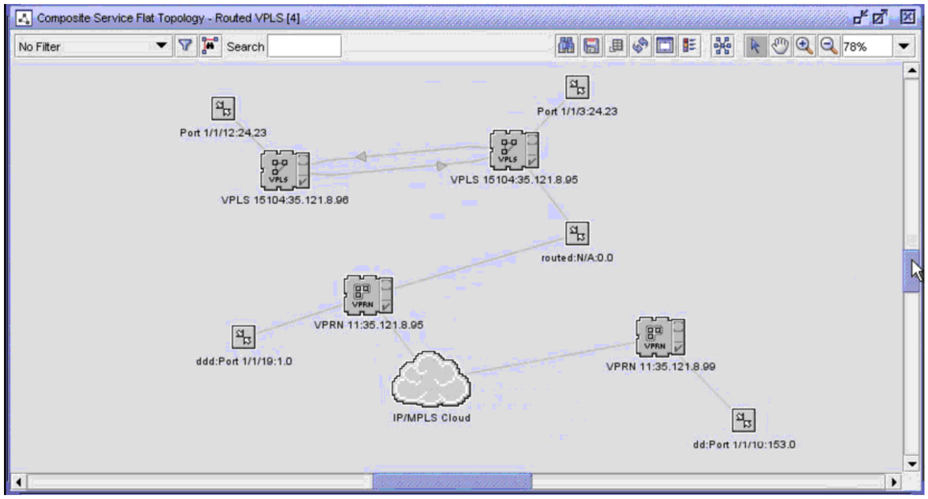
Figure 80-2 Composite service connected by spoke bindings



In this configuration, all four SAPs are considered as endpoints. Therefore MEPs are generated on each SAP and they all target each other. A total of twelve tests are generated. Double-clicking on an endpoint opens the interface configuration form and the MEP generated for this particular endpoint is displayed under the MEPs tab. If you then query the MEP's properties, the Tests tab in the MEP's configuration form displays the three tests that target the other MEPs in this composite service.

The second example is a routed VPLS configuration comprising a VPLS (VPLS 15104) and a VPRN (VPRN 11), and appears in Figure 80-3. The services are connected by a routed VPLS interface (shown as routed:N/A:0.0).

Figure 80-3 Routed VPLS composite service



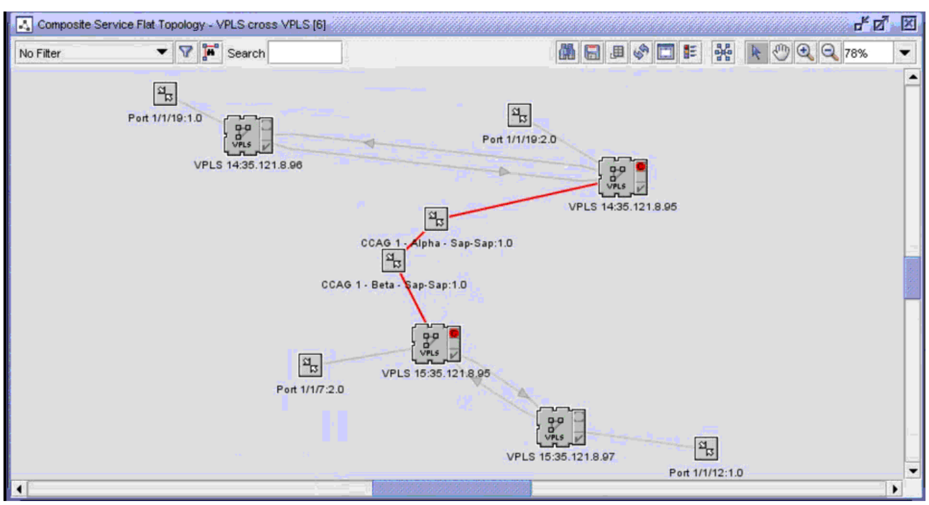
In this configuration, site 35.121.8.95 exists on both the VPLS and VPRN service. This is an overlapping site. The test generation rules would normally skip an overlapping site and no MEGs or tests would be generated for that site.

However in this case, the overlap for this site occurs in an unsupported service. The test generation rules for such a configuration will skip the unsupported VPRN service entirely and only generate tests for the supported VPLS, including site 35.121.8.95. Therefore, two MEPs and two tests (targeting each other) will be generated here, one for each of the SAPs on sites 35.121.8.96 and 35.121.8.95.

The test generation logs available in the test suite configuration form (under the Generation Logs tab) provide an explanation whenever the test generation rules cause items to be excluded from the tests. In this case, the log would state: “The CFM Composite Services Test Suite skipped the unsupported service”.

The third example is a cross-connected VPLS composite service configuration, and is shown in Figure 80-4.

Figure 80-4 Cross-connected VPLS composite service



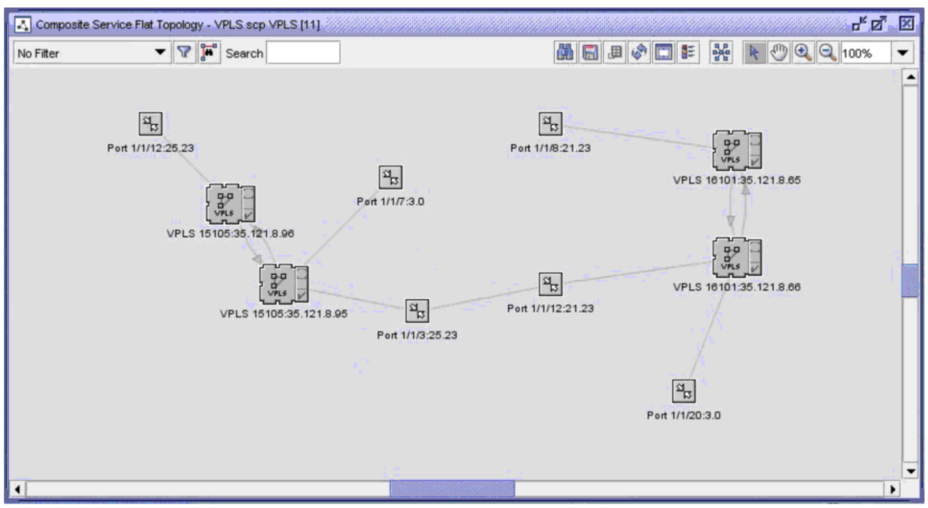
In this configuration, the two VPLSs (VPLS 14 and VPLS 15) are cross-connected by the SAPs CCAG 1-Alpha and CCAG 1-Beta. Both these SAPs originate from site 35.121.8.95, which exists in both services. It is therefore an overlapping site. The test generation rules skip overlapping sites, so no MEGs or tests are generated for any SAPs associated with that site.

Therefore, two MEPs and two tests (targeting each other) will be generated here, one for each of the SAPs on sites 35.121.8.96 and 35.121.8.97.

In addition, there will be two test generation logs available in the Generation Logs tab of the test suite configuration form. In this case, the logs would be identical, one stemming from each of the supported VPLSs. The logs would state: “Skipped overlapping service site”.

The fourth example is an SCP-connected VPLS composite service configuration, and is shown in Figure 80-5.

Figure 80-5 SCP-connected VPLS composite service



In this configuration, the two VPLSs (VPLS 15105 and VPLS 16101) are joined by an SCP connector between sites 35.121.8.95 and 35.121.8.66. The test generation rules skip any SAPs identified as part of a connector, since they are not endpoints. So no MEGs or tests are generated for either connector SAP.

MEGs and tests will however, be generated for each of the other four SAPs shown in the example. In total, four MEGs and twelve tests will be generated.

In addition, there will be two test generation logs available in the Generation Logs tab of the test suite configuration form. In this case again, the logs would be identical, one stemming from each of the supported VPLSs. The logs would state: “Skipped service connecting SAPs”.

80.2 Workflow to configure Ethernet CFM

This workflow describes the procedures to create and run an Ethernet CFM test.

Ethernet CFM tests are configured through the 5620 SAM Service Test Manager. See chapter 78 for more information.

1 Configure the initial MEP ID value on an NE for automatic MEP creation. See Procedure 80-2 for more information.

2 Create an Ethernet CFM MD and subordinate objects associated with the MD such as a Global MEG, MEG, and MEP for each level at which Ethernet connectivity is to be monitored. See Procedure 80-1 for more information.

- **i** Create one or more global MEGs in each MD. Each MEG must be associated with one service or Ethernet path. Creating a Global MEG generates a CFM continuity check test.
- **ii** Associate a service with the Global MEG.
- **iii** As required, add an Ethernet path to the Global MEG.
- **iv** As required, add a managed MEP to the MEG.
- **v** As required, add a remote MEP to the MEG.
- **vi** As required, add an unmanaged remote MEP to the Global MEG.
- **vii** As required, add a MEG sub-group to a Global MEG.

3 As required, change the MEG sub-group association for managed MEPs or unmanaged remote MEPs. See Procedure 80-3 for more information.

4 As required, configure a default NE-level MD on an OmniSwitch. See Procedure 80-4 for more information.

5 Create a test policy, specifying at least one of the following Ethernet CFM test definitions:

- CFM Loopback
- CFM Link Trace
- CFM Two Way Delay Test
- CFM Two Way SLM

See Procedure 78-4 for more information.

6 Create a test suite. See Procedure 78-8 for more information.

7 As required, execute the generated Ethernet CFM test suite. See Procedures 78-10 and 78-12 for more information.

8 As required, view the test results. See Procedures 78-13, 78-14, and 78-15 for more information.

80.3 Ethernet CFM procedures

The following procedures describe how to configure and manage Ethernet CFM.

Procedure 80-1 To configure an Ethernet CFM MD, and subordinate objects associated with the MD.

Perform this procedure to configure an Ethernet CFM MD, and subordinate objects associated with the MD such as a Global MEG, MEG, and MEP.

Note — This procedure assumes you have previously created a service to associate with the MD or subordinate objects.

1 Choose Tools→Ethernet CFM→Maintenance Domain from the 5620 SAM main menu. The Maintenance Domain Policies form opens.

2 Perform one of the following.

a To edit an existing MD, perform the following steps.

i Use the configurable filter to search for an MD and click on the Search button. A list of MD's appears.

ii Click on an MD and click on the Properties button. The Maintenance Domain Global Policy [Edit] form opens.

b To create a new MD, perform the following steps.

i Click on the Create button. The Maintenance Domain, Global Policy (Create) form opens.

ii Configure the parameters:

- MD Mgr Object ID
- Maintenance Domain ID
- Auto-Assign ID
- Name Type
- Name
- Level

If the MD is to be used for Y.1731 performance measurement tests, you must set the Name Type parameter to none.

iii Click on the Apply button. The form displays additional tabs, and the form name changes to Maintenance Domain Global Policy (Edit).

iv Click on the Switch Mode button. A dialog box appears to confirm that you want to continue.

v Click on the Yes button. The Configuration Mode changes to Released and the Maintenance Domain Global Policy [Edit] form reappears.

3 Configure the Description parameter and click on the OK button. A dialog box appears to confirm that you want to continue.

4 Click on the Yes button. The Maintenance Domain Global form reappears that lists the MD you created or edited.

5 To add a Global MEG to the MD, perform the following steps otherwise, go to step 18.

i Click on the MD you created or edited in step 2 and click on the Properties button. The Maintenance Domain Global Policy [Edit] form opens.

ii Click on the Global Maintenance Entity Group tab button.

iii Click on the Create button. The Global Maintenance Entity Group (Create) form opens with the General tab displayed.

iv Configure the following parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State
- Name Format
- Name
- Initial CCM Interval
- Initial MHF-Creation
- Initial CFM Hold Down Timer (centiseconds)

Note 1 — When the Initial CCM Interval parameter is set to 10 ms or 100 ms, you cannot configure automatic MEP creation in step 7.

Note 2 — The Initial CFM Hold Down Timer (centiseconds) parameter can only be configured when the Initial CCM Interval is 10 ms or 100 ms.

v Click on the OK button. The Global MEG is listed on the Maintenance Domain Global Policy [Edit] form and a default MEG sub-group is added to the Global MEG

6 To add a MEG sub-group to a Global MEG, perform one of the following, otherwise go to step 7.

a To add a new MEG sub-group to a Global MEG manually, perform the following steps:

i Click on the Global MEG you created or edited in step 5 and click on the Properties button. The Global Maintenance Entity Group [Edit] form opens with the General tab displayed.

ii Click on the MEG Sub-Group tab button.

iii Click on the Create button. The MEG Sub-Group (Create) form opens with the General tab displayed.

iv Configure the following parameters:

- MEG Sub-Group ID
- Auto-Assign ID
- Name
- Ignore test generation and CCM test

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The MEG sub-group is listed on the Global Maintenance Entity Group (Edit) form.

b To automatically create a new MEG sub-group based on existing remote MEP lists perform the following steps:

Note — MEG sub-groups can be created using this method only if a valid remote MEP list exists where remote MEPs are listening to each other.

i Click on the Global MEG you created or edited in step 5 and click on the Properties button. The Global Maintenance Entity Group [Edit] form opens with the General tab displayed.

ii Click on the More Actions button and choose Discover MEG Sub Groups. If a valid remote MEP lists exists where remote MEPs are listening to each other, new MEG sub-groups are created and listed on the Global Maintenance Entity Group (Edit) form, otherwise no action will be taken by 5620 SAM.

7 To associate a service with the Global MEG, perform one of the following.

Note — The differentiator between these two options is the action results in associating a service with the MEG on all nodes versus associating a service with the MEG on a single node.

a To automatically associate a service with the Global MEG on all nodes, perform the following steps:

i Click on the MD you created or edited in step 2 and click on the Properties button. The Maintenance Domain Global Policy [Edit] form opens.

ii Click on the Global Maintenance Entity Group tab button.

iii Click on the Create button. The Global Maintenance Entity Group (Create) form opens with the General tab displayed.

iv Click on the Service tab button.

v Click on the Create button. The Service (Create) form opens.

vi Click on the Select button. The Select Service form opens.

vii Click on the Search button. A list of services is displayed.

viii Select a service in the list and click on the OK button. The Select Service form closes, and the service information is displayed on the Service (Create) form.

ix As required, configure the following parameters:

- Auto MEG Site Creation
- MEP(s) Creation on Access Interfaces
- Direction
- MEP(s) Creation on SDP Bindings
- Direction
- Virtual MEP(s) Creation on B-Sites
- MIP(s) Creation on Access Interfaces
- MIP(s) Creation on SDP Bindings

Note — When the Initial CCM Interval parameter is set to 10 ms or 100 ms, you cannot configure the MEP(s) Creation on Access Interfaces, MEP(s) Creation on SDP Bindings, or Virtual MEP(s) Creation on B-Sites parameters.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The service is listed on the Global Maintenance Entity Group (Create) form.

b To associate a service with the Global MEG on a single node, perform the following steps.

i Click on the MD you created or edited in step 2 and click on the Properties button. The Maintenance Domain Global Policy [Edit] form opens.

ii Click on the Global Maintenance Entity Group tab button. A list of MDs appears.

iii Select an MD and click on the Properties button. The Global Maintenance Entity Group [Edit] form appears.

iv Click on the Maintenance Entity Group tab button.

v Click on the Create button. The Maintenance Entity Group (Create) form opens.

vi Click on the Select button. The Select Site form opens.

vii Click on the Search button. A list of sites is displayed.

viii Select a site in the list and click on the OK button. The Select Site form closes, and the service information is displayed on the Maintenance Entity Group (Create) form.

ix Click on the Service tab button and click on the Create button. The MEG Service [Create] forms opens.

x Configure the following parameters:

- CCM interval
- VLAN ID
- MHF-Creation

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The service is listed on the Global Maintenance Entity Group (Create) form.

8 Perform the following steps to add an Ethernet path to the Global MEG, if required.

i Click on the Ethernet Path tab button.

ii Click on the Create button. The Ethernet Path (Create) form opens.

Note — You must specify an Ethernet tunnel path or Ethernet ring path on this form.

iii To add an Ethernet tunnel path, click on the Select button in the Ethernet Tunnel Path panel. The Select Ethernet Tunnel Path form opens. Otherwise, go to step 8 vi.

iv Select an Ethernet tunnel path in the list and click on the OK button. The Select Ethernet Tunnel Path form closes, and the Ethernet tunnel path is displayed on the Ethernet Path (Create) form.

v Go to step 8 viii.

vi Click on the Select button in the Ethernet Ring Path panel. The Select Ethernet Ring Path form opens.

vii Select an Ethernet ring path in the list and click on the OK button. The Select Ethernet Ring Path form closes, and the Ethernet ring path is displayed on the Ethernet Path (Create) form.

viii Configure the parameters:

- Auto-Assign ID
- Object ID
- Run Continuity Check Protocol
- Set Control MEP property on created MEPs

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Ethernet path is displayed on the Global Maintenance Entity Group (Create) form.

9 Perform the following steps to add a MEG to the MD.

i Click on the Maintenance Entity Group tab button.

ii Click on the Create button. The Maintenance Entity Group (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Site form opens.

iv Select an NE in the list and click on the OK button. The Select Site form closes, and the Maintenance Entity Group (Create) form displays the NE information.

v Configure the parameters:

- CCM interval
- VLAN ID
- MHF-Creation
- CFM Hold Down Timer (centiseconds)

> **Note —** The MHF-Creation and VLAN ID parameters are configurable only when the selected NE is an OmniSwitch.
>
> The CFM Hold Down Timer (centiseconds) parameter can only be configured when the CCM interval is 10 ms or 100 ms.

vi To associate a template with the MEG, click on the Templates tab button. Otherwise, go to step 9 ix.

vii Click on the Select button. The Select Associated Template - Maintenance Entity Group form opens.

viii Select a template in the list and click on the OK button. The Select Associated Template - Maintenance Entity Group form closes, and the Maintenance Entity Group (Create) form displays the template information.

ix Click on the Service tab button. A list of services is displayed.

x Click on the Create button. The MEG Service (Create) form opens.

xi Configure the parameters:

- Service ID
- MHF-Creation
- VLAN ID
- Id-Permission

xii Click on the OK button. The MEG Service (Create) form closes.

xiii Click on the Apply button. A dialog box appears.

xiv Click on the OK button. The form name changes to Maintenance Entity Group (Edit), and the service is listed on the form, which displays additional tab buttons.

10 Perform the following steps to add a managed MEP to the MEG, if required.

i Click on the Managed MEP tab button.

ii Click on the Create button. The MEP (Create) form opens.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Interface Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

Note — The Interface Type parameter is configurable when the Type parameter is set to Regular.

iv If the Type parameter is set to Virtual, go to step 9 ix.

v Click on the Select button in the bottom panel to choose an object of the type specified by the Interface Type parameter. The Select *object_type* form opens.

vi Click on the Search button. A list of objects is displayed.

vii Select an object in the list and click on the OK button. The Select *object_type* form closes, and the object information is displayed on the MEP (Create) form.

viii Go to step 9 ix.

ix Click on the Select button in the bottom panel to choose a site for the virtual MEP. The Select Service Site Pointer form opens.

x Click on the Search button. A list of sites is displayed.

xi Select a site in the list and click on the OK button. The Select Service Site Pointer form closes, and the site information is displayed on the MEP (Create) form.

xii If the MD has a Name Type of none and the Global MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable. Otherwise, go to step 9 xxiv.

xiii Click on the Y.1731 Tests tab button.

xiv Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xv Click on the AIS tab button.

xvi Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xvii Click on the OK button. A dialog box appears.

xviii Click on the OK button. The MEP (Create) form closes, and the managed MEP is listed on the Maintenance Entity Group (Edit) form.

11 Perform the following steps to add a remote MEP to the MEG, if required.

Note 1 — You can add only one entry to the remote MEP list for a 7705 SAR.

Note 2 — When you execute a CCM test or synchronize the managed and unmanaged remote MEP lists, the 5620 SAM automatically distributes the local MEP and the remote MEP to the remote MEP list, except for 7705 SAR NEs, which are excluded from automatic MEP -distribution.

Note 3 — When you execute a CCM test or synchronize the managed and unmanaged remote MEP lists within a MEG sub-group, the 5620 SAM automatically distributes the local MEP and the remote MEP within that MEG sub-group.

Note 4 — If a local MEP and the corresponding remote MEP are on the same OmniSwitch, deleting the remote MEP results also deletes the corresponding local MEP.

i Click on the Remote MEP tab button. The Remote MEP (Create) form opens.

ii Configure the MEP ID parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The remote MEP is listed on the Maintenance Entity Group (Edit) form.

12 Click on the OK button. The Maintenance Entity Group (Edit) form closes, and the MEG is listed on the Global Maintenance Entity Group (Edit) form.

13 Perform the following steps to add an unmanaged remote MEP to the Global MEG, if required.

i Click on the Unmanaged Remote MEP tab button.

ii Click on the Create button. The Unmanaged Remote MEP (Create) form opens.

iii Configure the parameters:

- MEP ID
- MEP Mac Address

iv Click on the Select button in the bottom panel to associate the unmanaged remote MEP to a MEG sub-group. The Select MEG Sub-Group form opens.

v Click on the Search button. A list of MEG sub-groups is displayed.

vi Select a MEG sub-group in the list and click on the OK button. The Select MEG Sub-Group form closes, and the MEG sub-group information is displayed on the Unmanaged Remote MEP (Create) form.

Note — If a MEG sub-group is not selected, the unmanaged remote MEP is automatically associated with the default MEG sub-group.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The unmanaged remote MEP is listed on the Global Maintenance Entity Group (Edit) form.

14 Perform the following steps to add a managed MEP to the Global MEG, if required.

i Click on the Managed MEP tab button.

ii Click on the Create button. The MEP (Create) form opens.

iii Click on the Select button. The Select Maintenance Entity Group form opens.

iv Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

v Click on the Select button in the bottom panel to associate the managed MEP to a MEG sub-group. The Select MEG Sub-Group form opens.

vi Click on the Search button. A list of MEG sub-groups is displayed.

vii Select a MEG sub-group in the list and click on the OK button. The Select MEG Sub-Group form closes, and the MEG sub-group information is displayed on the MEP (Create) form.

Note — If a MEG sub-group is not selected, the managed MEP is automatically associated with the default MEG sub-group.

viii Configure the parameters:

- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Interface Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

Note 1 — The Interface Type parameter is configurable when the Type parameter is set to Regular.

Note 2 — The Interface Type Port is only available if the MD level is 0.

Note 3 — For facility MEPs, the Direction parameter must be set to Down.

ix If the Type parameter is set to Virtual, go to step 14 xvi.

x If the Interface Type is set to LAG or Port, configure the Facility Fault Notify parameter.

xi If the Interface Type is set to LAG, configure the Facility VLAN ID.

Note — If you are configuring a tunnel facility MEP, Facility VLAN ID must match the outer encapsulation value of the SAP to which you are connecting the tunnel facility MEP.

xii Click on the Select button in the bottom panel to choose an object of the type specified by the Interface Type parameter. The Select *object_type* form opens.

xiii Click on the Search button. A list of objects is displayed.

xiv Select an object in the list and click on the OK button. The Select *object_type* form closes, and the object information is displayed on the MEP (Create) form.

xv Go to step 14 xix.

xvi Click on the Select button in the bottom panel to choose a site for the virtual MEP. The Select Service Site Pointer form opens.

xvii Click on the Search button. A list of sites is displayed.

xviii Select a site in the list and click on the OK button. The Select Service Site Pointer form closes, and the site information is displayed on the MEP (Create) form.

xix If the MD for the MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable. Otherwise, go to step 14 xxv.

xx Click on the Y.1731 TEST tab.

xxi Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

  The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xxii Click on the AIS tab.

xxiii Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

  The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xxiv Click on the OK button. A dialog box appears.

xxv Click on the OK button. The MEP is listed on the Global MEG (Create) form.

15 Click on the Synchronize Remote MEPs button to distribute the MEPs to the NEs.

Note — If the managed MEP or unmanaged remote MEP belongs to a MEG sub-group, the remote MEP synchronization will only occur within the MEG sub-group.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Global MEG (Create) form closes, and the Maintenance Domain (Edit) form reappears.

18 Close the Maintenance Domain (Edit) form.

19 Close the Manage Maintenance Domain Policies form.

Procedure 80-2 To configure automatic MEP ID assignment on an NE

Perform this procedure to configure an initial MEP ID value on an NE for automatic MEP creation.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the device where you want to configure automatic MEP ID assignment and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Configure the MEP Id parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The NE properties form closes.

Procedure 80-3 To change the MEG sub-group association for managed MEPs or unmanaged remote MEPs

Perform this procedure to change the MEG sub-group association for managed MEPs or unmanaged remote MEPs.

1 Select Manage→Service→Services. The Manage Services form opens.

2 Click on the Search button. A list of services is displayed.

3 Select a service in the list and click on the Topology View button. The Service Topology map opens.

4 Select the OAM check box at the bottom left of the map window. MEG and MEP objects are added to the map.

5 Right-click the interface object that includes the MEP that you wish to move to another MEG sub-group and choose Ethernet CFM→Edit MEP from the contextual menu.The Select MEP (Edit) form opens.

6 In the MEG Sub-Group panel, click on the Clear button to remove the current MEG sub-group association.

7 Click on the Select button. The Select MEG Sub-Group form opens.

8 Click on the Search button. A list of MEG sub-groups is displayed.

9 Click on an MEG sub-group and click on the OK button. The Select MEG Sub-Group form closes and the MEG sub-group information is displayed in the MEG Sub-Group panel.

10 Select OK. The MEP (Edit) form closes, the MEP object color changes, and the MEP is moved to the newly selected MEG Sub-Group.

Procedure 80-4 To configure a default MD on an OmniSwitch

Perform the following procedure to configure a default NE-level MD on an OmniSwitch.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch NEs icon.

3 Right-click on the device where you want to configure a default MD and select Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Click on the Globals tab button.

5 Click on the CFM tab button.

6 Configure the parameters:

- Level
- MHF-Creation
- Id-Permission

7 Close the Network Element (Edit) form.

81 — RCA audit

81.1 RCA audit overview

The 5620 SAM RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the 5620 SAM provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.

Note — The adjustments are made only to the 5620 SAM database and are not deployed to the network.

You can perform RCA audits of the following objects:

- VLL services
- VPLSs
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (5620 SAM/5650 CPAM integration only)
- IS-IS interfaces and sites (5620 SAM/5650 CPAM integration only)

Note — You need the 5650 CPAM license to perform the OSPF and IS-IS RCA audits. See the *5650 CPAM User Guide* for more information.

5620 SAM service audit

A 5620 SAM service is defined as a collection of service sites with the same customer ID, service type, and service ID. The 5620 SAM discovers services that are configured on a 7750 SR, 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7210 SAS-E using the service ID on the NE. Configuration errors may occur in networks where the services were created and deployed on the NEs using CLI before the NEs were managed by the 5620 SAM.

For example, when two VPLSs with the same service ID and the same mesh VC ID on an NE are discovered by the 5620 SAM, they are discovered as a single service in the 5620 SAM.

Another example of a configuration error is when a switching Epipe has multiple Epipe sites and multiple VC IDs for different segments. If different service IDs are used when the sites are created, the 5620 SAM assumes that the sites are connected and creates multiple VLL services within a composite service.

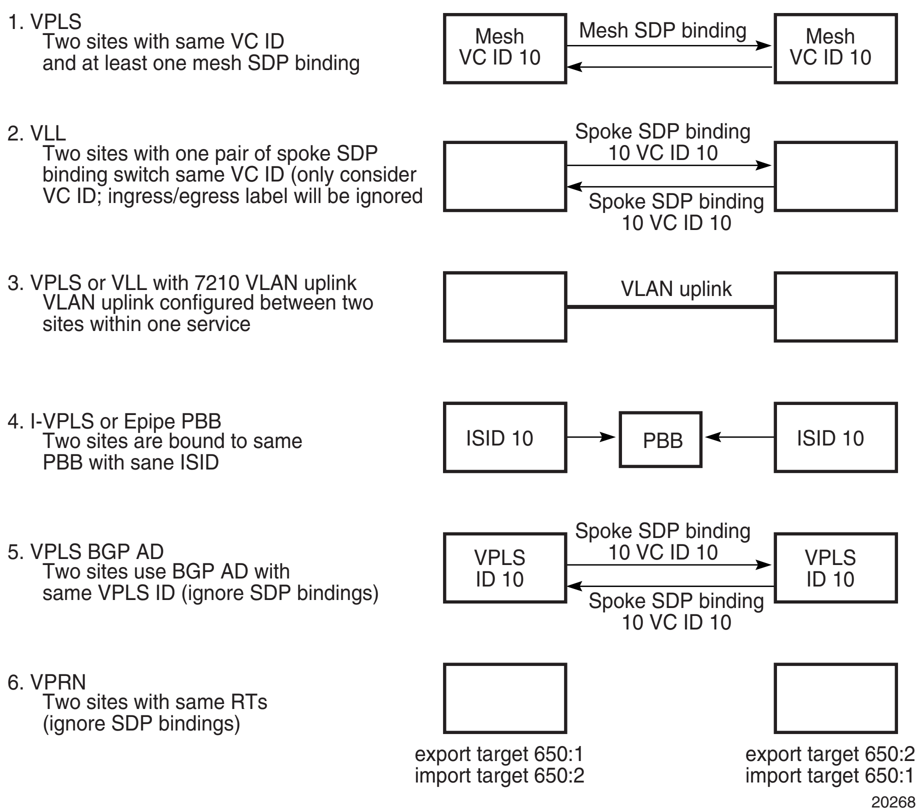
RCA audit policies allow you to modify the component membership of your 5620 SAM services to detect possible configuration problems. In addition, you can use the RCA audit to correct most configuration problems that are discovered in the audit.

Note — A 5620 SAM user that is assigned the Administrator or RCA scope of command role can create, modify, and execute all RCA audit policies. A 5620 SAM user that is assigned the Administrator or Service scope of command role can execute service audit adjustments.

Service membership rules

The 5620 SAM uses the rules in Figure 81-1 to identify whether two service sites are connected together. When two sites are identified as connected, they should belong to same service.

Figure 81-1 Rules to check whether two sites are connected



If service sites have different customer IDs, the 5620 SAM discovers the sites as belonging to different services. After the audit, the 5620 SAM generates a problem for each service. You can specify to which service the 5620 SAM should move the site and whether the empty service should be removed after the sites are moved.

For VPLS or VLL services, if the same service ID is used for two groups of sites that are not connected, the 5620 SAM detects a duplicate service ID. Two problems are generated for one of the group of sites, and the solution is to separate the services. If there are other groups of isolated sites, additional problems are generated for each group.

Consider the following when you perform an audit of a VPLS.

- Although different service IDs may be used, I-sites that are bound to same backbone VPLS and have the same ISID are considered to be in the same VPN.
- For VPLS sites that use BGP auto-discovery, the VPLS ID is used to determine service membership.
- H-VPLS is discovered as composite service in the 5620 SAM if different service IDs are used.

Consider the following when you perform an audit of a VLL service.

- Service sites with different customer IDs are discovered as two services, and can reconfigured as one service.
- More than two groups of sites that are connected can be detected and can be separated into different services.
- Redundant VLLs are not be affected by the audit and are considered correctly configured.
- If two Epipe sites are connected to the same PBB with same B-VPLS service ID, and the source and destination MAC addresses match, the 5620 SAM determines that the two sites are connected. If they are in different 5620 SAM services, a problem is generated during the audit.

Consider the following when you perform an audit of a VPRN service.

- VPRN service membership is based on the RTs defined in the VRFs.
- Sites that are in different services but have common import and export route targets. Import target of Site 1 is equal to the Export target of Site 2.

Physical link audits

Physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the equipment window, physical topology map, and the Manage Equipment list form of the 5620 SAM, on each router using the CLI. Because several key parameters on each end of the physical link depend on each other, configuration errors are possible. The 5620 SAM RCA audit tool allows you to identify configuration errors in physical links. The 5620 SAM does not provide a solution for configuration problems that the RCA audit identifies for physical links. By default, the RCA audit detects the following configuration errors in physical links:

- **physical port parameters**
    - mismatched MTU values
    - mismatched speeds
- **Ethernet port parameters**
    - Auto-negotiate parameter misconfiguration
    - Duplex parameter misconfiguration

You can configure the RCA audit policy for the physical link to include additional physical link properties in the audit.

Viewing and analyzing RCA audit results

The RCA Audit Problem(s) indicator on the General tab of a network object properties form identifies whether configuration problems were detected in previous audits. The Last Audit Time indicator displays a timestamp of the last audit that was performed. The RCA Audit command is accessed from the More Actions button at the bottom of the service properties form.

After you associate an audit policy with the object, you can perform an RCA audit and view the results. If no problems are detected, the RCA Result tab does not appear.

The properties form of a problem displays the following information:

- problem severity
- probable cause
- description
- solution

The Caused By Objects tab lists the network objects that caused the problem. For service audits, the sites that should be moved out of a service, and the service they should move to, if there is only one destination service, are listed. If only one group of sites is listed, a new service is created and the sites are moved to the created service.

Table 81-1 describes the probable causes of problems.

Table 81-1 Probable causes

Probable cause	Description
Unknown	The probable cause could not be determined.
Underlying Resource Operational Down	The underlying resource of the object is operationally down.
Misconfiguration	There is a misconfiguration error.
Admin Down	The object is administratively down.
Underlying Resource Admin Down	The underlying resource of the object is administratively down.
Underlying Resource Missing	An underlying resource is missing.
Underlying Resource Problem	Problem with an underlying resource
Aggregated	Aggregated cause
Service Membership Misconfigured	The service membership is not configured correctly.

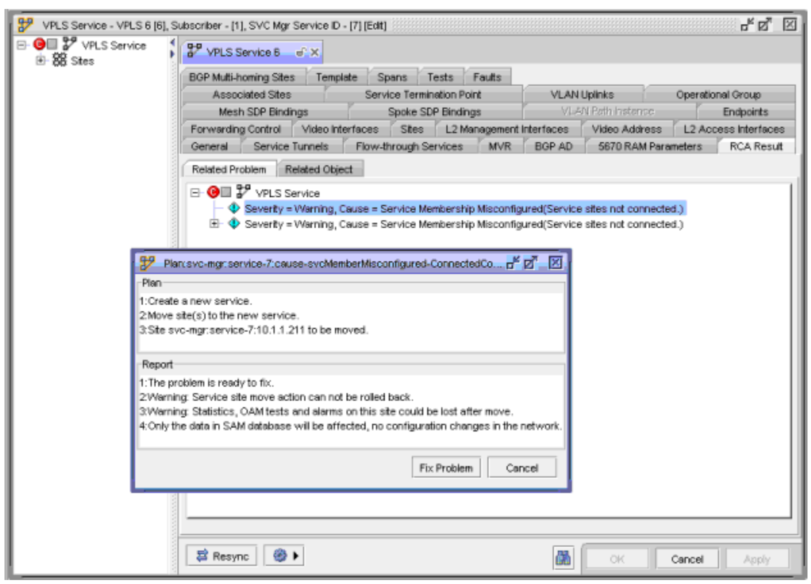
(1 of 2)

Probable cause	Description
Route Targets are misconfigured for VPLS BGP Multi-homing	One of the following misconfigurations exists: • No matching RT for peered multi-homing sites • There are multiple RTs configured for a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies or multiple services. • Multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
No valid Route Targets configured for VPLS BGP Multi-homing	No valid Route Targets currently exist for a VPLS site that has BGP multi-homing sites configured under it.
No members configured for this Multi-homing site	The BGP VPLS multi-homing site does not have other sites as members that share the same multi-homing ID in order to comprise a group.

(2 of 2)

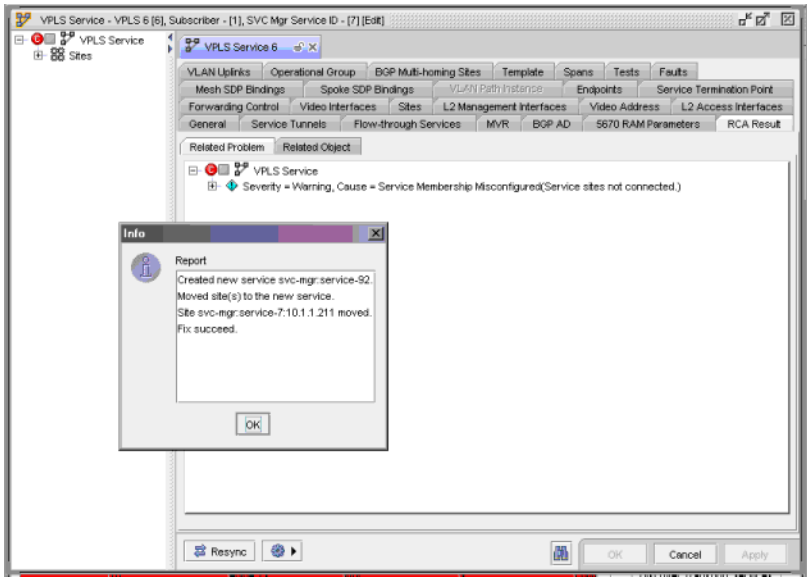
You can use the RCA audit tool to correct a detected configuration problem from the RCA Result tab on the network object properties form. The 5620 SAM lists the operations to fix the problem, as shown in Figure 81-2.

Figure 81-2 Correction plan for a problem



When you accept the proposed solution, a summary of the correction operation that the 5620 SAM implemented appears, as shown in Figure 81-3. To view the result in the server or client log, you must enable the logging option in the nms-server.xml or nms-client.xml file.

Figure 81-3 Correction report



81.2 Workflow to configure RCA audit

1. Create or configure an RCA audit policy. For service audits, configure one or more audit policies for each service type to detect different configuration problems. See Procedure 81-1 for more information.

2. Run the RCA audit policy for a specific service or object.

   a. Perform an RCA audit of a VLL service. See Procedure 81-2 for more information.

   b. P.erform an RCA audit of a VPLS. See Procedure 81-3 for more information.

   c. Perform an RCA audit of a VPRN service. See Procedure 81-4 for more information.

   d. Perform an RCA audit of multiple services. See Procedure 81-5 for more information.

   e. Perform an RCA audit of a physical link. See Procedure 81-6 for more information.

3. Alternatively, create a service audit to run at a scheduled time. See Procedure 81-7 for more information.

4. Identify the problems and view the suggested solutions. Solutions are not provided for physical links.

5. Implement the changes, as required.

81.3 RCA audit procedures

Use the following procedures to perform RCA audit tasks.

Procedure 81-1 To configure an RCA audit policy

1 Choose Policies→Network and Service Audits from the 5620 SAM main menu. The Network and Service Audits form opens.

2 Select Audit Policy (RCA) from the drop down list.

3 Perform one of the following.

   a To create an RCA audit policy, click on the Create button. The Audit Policy (Create) form opens with the General tab displayed.

   b To configure an existing RCA audit policy, click on the Search button and choose an entry from the list. Click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed. Go to step 5.

4 If you are creating an RCA audit policy, configure the following parameters. Otherwise, go to step 5.

- Auto-Assign ID
- ID

5 Configure the Description parameter.

6 If you are creating an RCA audit policy, click on the Select RCA Policy To Run The Audit button. Otherwise, go to step 11. The RCA Policy form opens.

7 Choose one of the following options:

- RCA Audit Physical Link
- RCA Audit ISIS
- RCA Audit OSPF
- RCA Audit VLL
- RCA Audit VPLS
- RCA Audit VPRN

Note — You require a 5650 CPAM license to create an RCA Audit ISIS or RCA Audit OSPF policy.

8 Double-click on an entry to modify the policy description, if required.

9 Click on the OK button. The RCA Policy form closes.

10 Click on the Apply button.

11 Click on the Entry tab button. Depending on the option specified in step 7, a list of RCA audit policy entries is displayed.

The RCA audit policy entry for a VLL RCA audit is: RCA Audit for VLL Service Membership.

The RCA audit policy entry for a VPRN RCA audit is: RCA Audit for VPRN Service Membership.

The following are the RCA audit policy entries for a VPLS RCA audit:

- RCA Audit for VPLS Service Membership
- RCA Audit for B-VPLS PBB
- RCA Audit for BGP Multi-homing

The following are the RCA audit policy entries for a physical link RCA audit:

- RCA Audit For Physical Ports of Physical Links
- RCA Audit For Ethernet Port Specifics of Physical Links

12 Choose an entry from the list and click on the Properties button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form opens with the General tab displayed.

13 Configure the parameters:

- Enabled
- Remove Empty Service

14 If you are configuring an RCA audit policy for physical links, perform the following steps. Otherwise, go to step 15.

i Click on the Attributes tab button. A list of default attributes for the physical link entry is displayed.

ii Perform one of the following:

- To configure default attributes, go to step iii.
- To add an attribute, go to step v.

iii Activate or deactivate the RCA audit for each attribute by enabling or disabling the check box in the Enabled column.

iv Choose one of the problem severity options for each attribute by clicking on the entry in the Severity column of the attribute. A contextual menu appears.

- Minor
- Conditional
- Info
- Critical
- Major
- Warning
- Indeterminate

v Click on the Add button to add an attribute. Otherwise, go to step 15. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form opens with a list of attributes associated with the physical link entry.

vi Choose one or more attributes in the list and click on the OK button. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form closes and the Audit Policy Entry - RCA Audit Policy - RCA Audit For *entry_type* of Physical Links (Edit) form refreshes with the attribute information.

15 Click on the OK button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form closes.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Audit Policy (Edit) form closes.

18 Close the RCA Audit Policy form.

Procedure 81-2 To perform an RCA audit of a VLL service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VLL from the object drop-down list.

3 Click on the Search button. A list of VLL services appears.

4 Choose an entry from the list and click on the Properties button. The *VLL_type* (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VLL Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab button to view related problems.

14 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tab buttons to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the *VLL_type* (Edit) form.

23 Close the Manage Services form.

Procedure 81-3 To perform an RCA audit of a VPLS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Search button. A list of VPLS services appears.

> **Note —** In addition to the standard audit checks, for BGP VPLS multi-homing sites the audit also checks:
>
> - if no valid Route Targets are configured under a VPLS site that has BGP multi-homing sites configured under it.
> - if there are no matching RTs for peered multi-homing sites
> - if there are multiple RTs configured under a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies (or multiple services, since the RT defines the service)
> - if multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
> - if a multi-homing site does not have other sites as members (sharing the same multi-homing ID to comprise a group)

3 Choose an entry from the list and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

5 Click on the More Actions button and choose RCA Audit. The Select RCA Policy to run the audit list form appears with a list of configured policies.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and the requested audit is performed. A dialog box appears.

7 Click on the OK button.

8 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

> **Note —** The RCA Result tab appears only if the RCA audit detects one or more problems.

9 If required, expand the VPLS Service object in the problems tree to view the problems, the associated severity, and the cause.

10 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

11 Configure the Disable Fix Window parameter.

12 Click on the Related Problem tab button to view related problems.

13 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tab buttons to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 11.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

21 Close the VPLS Service (Edit) form.

22 Close the Manage Services form.

Procedure 81-4 To perform an RCA audit of a VPRN service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VPRN from the object drop-down list.

3 Click on the Search button. A list of VPRN services appears.

4 Choose an entry from the list and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VPRN Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab button to view related problems.

14 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tab buttons to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

> **Note —** The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the VPRN Service (Edit) form.

23 Close the Manage Services form.

Procedure 81-5 To perform an RCA audit of multiple services

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose one of the following from the object drop-down list.

- AbstractVpls (VPLS)
- VPRN Service (VPRN)
- Vll (VLL)

3 Click on the Search button. A list of services appears.

4 Select the services that you want to audit.

5 Click on the RCA Audit button. The Select RCA Policy list form opens.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears with the following information:

- number of services audited
- number of successful audits
- number of problems generated

7 Click on the OK button.

8 Scroll to the RCA Audit Problem column and set the filter to = true.

9 Click on the Search button. A list of services with problems appears.

10 Select a service and click on the OK button. The *Service* (Edit) form appears with the General tab displayed.

11 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

12 If required, expand the *Service* object in the problems tree to view the problems, the associated severity, and the cause.

13 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

14 Configure the Disable Fix Window parameter.

15 Click on the Related Problem tab button to view related problems.

16 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

17 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

18 Click on the tab buttons to view information about the configuration.

19 Configure the parameters, as required.

20 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

21 Click on the Yes button.

22 Close the Problem (Edit) form.

23 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 14.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

24 Close the *Service* (Edit) form.

25 Close the Manage Services form.

Procedure 81-6 To perform an RCA audit of a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Click on the Select Object Type button and choose one of the following from the object tree.

- Physical Link (Network)
- Discovered Physical Link (Network)

3 Click on the Search button. A list of physical links appears.

4 Choose an entry from the list and click on the Properties button. The Physical Link (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the More Actions button and choose RCA Audit. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the Physical Link object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Click on the Related Problem tab button to view related problems.

Note — The 5620 SAM does not provide a solution for physical link configuration errors.

13 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tab buttons to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 Close the Physical Link (Edit) form.

21 Close the Manage Equipment form.

Procedure 81-7 To create a service audit scheduled task

1 Choose Policies→Network and Service Audits from the 5620 SAM main menu.

2 The RCA Audit Policy form opens.

3 Specify a filter for the search, if required, and click on the Search button. A list of RCA audit policies appears.

4 Choose a service audit policy from the list and click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed.

5 Click on the Schedule button and choose Create Service Audit Schedule Task. The Service Audit Scheduled Task (Create) form opens.

6 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

7 Click on the Select button in the Schedule panel. The Select Schedule - Service Audit Scheduled Task form opens.

8 Perform one of the following.

a Create a schedule to associate with the scheduled task.

b Associate an existing schedule to the scheduled task. Go to step 10.

9 Create a schedule.

i Configure the parameters:

- Name
- Description
- Current Client Start Time
- Current Client End Time
- Delay Time (seconds)
- Enable
- Ongoing
- Frequency

The Current Client End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the Current Client End Time expires.

ii Perform the step that corresponds to the Frequency parameter value specified in step i.

- When the parameter is set to Once, go to step iii.
- When the parameter is set to Per Second, configure the following parameters:
  - Run Every Second
  - Run Every Seconds
- When the parameter is set to Per Minute, configure the following parameters:
  - Run Every Minute
  - Run Every Minutes
- When the parameter is set to Per Hour, configure the following parameters:
  - Run Every Hour
  - Run Every Hours
- When the parameter is set to Per Day, configure the following parameters:
  - Run Every Day
  - Run Every Days
  - Run Every
- When the parameter is set to Per Week, configure the following parameters:

  Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Week
  - Run Every Weeks
  - Run Every
- When the parameter is set to Per Month, configure the following parameters:

  Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Month
  - Run Every Months
  - Run Every

iii Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Select Schedule - Service Audit Scheduled Task form reappears.

10 Choose an entry from the list and click on the OK button. The Select Schedule - Service Audit Scheduled Task form closes and the Service Audit Scheduled Task (Create) form reappears.

11 Ensure that the Administrative State parameter is set to Enabled.

12 Click on the OK button. The Service Audit Scheduled Task (Create) form closes. The RCA Audit Policy form reappears with additional tab buttons.

13 To apply a filter to the schedule, perform the following.

i Click on the Schedule Filter tab button.

ii Click on the Select button in the Audit Filter panel. The Select Audit Filter - Audit Policy form opens.

iii Click on the Search button. A list of filters appears.

Note — If no filters appear, click on the Audit Filter button to create a new filter. See chapter 3 for more information about how to create a filter.

iv Choose an entry and click on the OK button. The Select Audit Filter - Audit Policy form closes and the Audit Policy (Edit) form reappears with additional tab buttons.

14 Click on the Scheduled Objects to be Audited tab button to view the services that are included in the audit.

15 Click on the Scheduled Result tab button to view the results of the scheduled audit.

16 Click on the Problems tab button to view the problems associated with the audit.

17 Close the Audit Policy (Edit) form.

18 Close the RCA Audit Policy form.

Appendices

A. Scope of command roles and permissions

A.1 Predefined scope of command profiles and roles

This appendix describes the predefined 5620 SAM scope of command profiles and roles, and the permissions for each predefined role. Predefined scope of command profiles and roles cannot be deleted.

Predefined scope of command profiles

Table A-1 lists the predefined scope of command profiles, the assigned roles for each profile, and a description for each profile.

Table A-1 Predefined scope of command profiles

Profile name	Assigned roles	Description
admin	Administrator	Default administrative scope of command profile with access to all objects from the 5620 SAM GUI. This profile has no OSSI access.
SAMqa	Administrator OSS Management	Default OSSI administrative scope of command profile.

Predefined scope of command roles

Table A-2 lists the predefined scope of command roles for 5620 SAM user security and provides a description for each role.

Table A-2 Predefined scope of command roles

Role	Access provided
Base Read-only	Read-only to all objects except for the objects in the SAM Security and Mirror Service Management roles.
Administrator	GUI access, but no OSSI access, to all objects.
User Management	5620 SAM user and group management.
SAM Management and Operations	Database functions such as backup, restore, reinstantiation, and switchover. Alarm administration such as acknowledgement, clearing, and setting severity-change thresholds. General NE management functions such as discovery, deployment, mediation, polling, statistics management, and security management that includes modifying spans.
Network Element Equipment Management	Physical equipment configuration and management.
Service Management	Service, service component, and service template management functions, excluding mirror-service management.
Old Service Template Management	Management of service templates deprecated; see Template Script Management in this table.
Subscriber Management	Customer and residential subscriber management.

(1 of 3)

Role	Access provided
QoS/ACL Policy Management	General QoS and ACL policy management, Ethernet service and time of day suite policy management.
Policy Management (except QoS/ACL)	Management of policies other than those in the QoS/ACL Policy Management role.
Routing Management	Routing protocol, L2 forwarding, and bandwidth management.
Tunnel Management	Service tunnel and underlying transport management.
SAM Management and Operations	Database management (Backups, Reinstantiation, and Switchovers), Alarm acknowledgement, Alarm clearing, and Severity Change Thresholds, Router administration (Scheduling, Backup Policies, Upgrade Policies, Deployment Policies, and Management Ping Policies), NE Security, LPS, and Mediation Policies, SNMP Poller/Stats Polices, Event Notification Policies, MIB Policies, SNMP Performance Statistics, SAM Performance Statistics, Statistics Plotter, Usage and Activity Records, as well as Span configuration.
Network Element Software Management	NE software management functions.
Fault Management	Functions such as alarm management and remote network monitoring.
Service Test Management	STM functions such as creating, running and scheduling OAM tests.
Script Management	XML API and CLI script management, excluding execution.
Script Execution	XML API and CLI script execution.
Mirror Service Management	Creation and management of mirror services and mirror-service components using the GUI.
OSS Management	Use of the OSSI.
Telnet/SSH Management	Telnet or SSH access to NEs from the GUI.
CPAM Management	Route Analysis of ISIS Topology, OSPF Topology, MPLS Topology, IP Path monitoring, LSP Monitoring, Checkpoints, and Impact Analysis Scenarios for CPAM managment.
CPAM OSS PCA	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM routing.
CPAM Topology Simulator	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM Topology Simulator.
Root Cause Analysis (RCA) Object Verification	RCA functions.
Lawful Interception Management	LI configuration for mirror services, mediation policies, and NE security.
Template Script Management	Service and tunnel template script management.
Service Template Script Execution	Service template script execution.
Tunnel Template Script Execution	Tunnel template script execution.
Application Assurance (AA) Management	AA policy management.
Format and Range Policy Management	Format and range policy management, service-creation span rules.
Work Order Activation	The ability to perform CM work order activation.
Configuration Snapshot Export	The ability to perform export CM configuration snapshots.
Create and Delete Access	The ability to create and/or delete eNodeB objects via 5620 SAM-O.
Configuration Management which causes node reset	The ability to configure objects which causes a full or partial reset of the node.
EPC Operator	Read and write permission on all Evolved Packet Core classes.

(2 of 3)

Role	Access provided
eNodeB NEM Operator	The ability to launch the 9400 NEM (parameter configuration tool for the eNodeB) from the 5620 SAM client GUI.

(3 of 3)

A.2 Permissions

Table A-3 lists the permissions that can be assigned to a 5620 SAM scope of command role and provides a functional description for each permission.

Table A-3 Permissions

Package.Class.Method/Property	Description
aapolicy	Application Assurance - AA policies, configuration, protocol, group, filter, and profiles.
accessuplink	Access Uplink - Configuration of 7210 Access Uplink Specifics for physical ports and LAG interfaces.
accounting	Accounting Policy - Statistics Accounting Policies.
aclfilter	ACL Filter Policy - MAC, IP, and IPv6 ACL Filters.
activation	Activation - Used to define, manage, and deploy work orders used in activation.
activation.Session	Activation Session - Used to manage activation sessions and activate work orders.
activation.Snapshot	Snapshot - Used to manage CM configuration snapshots.
activation.SnapshotEntity	Snapshot Entity - Used to manage snapshot entities.
activation.WebDAVSharedData	Activation. Web DAVShared Data - Ability to restrict access to CM data (CM work orders and configuration snapshots) via the WebDAV protocol.
activation.WorkOrder	Work Order - Used to manage work orders.
aengr	Access Egress Policy - Access Egress QoS Policies.
aingr	Access Ingress Policy - Access Ingress QoS Policies.
ancp	ANCP - Access Node Control Protocol (ANCP) policy and configuration.
ancp.AncpLoopback	ANCP Loopback - Access to ANCP Loopback tests, ANCP Loopback test definitions, and ANCP Loopback deployed tests.
antispoof	Anti-Spoofing - Anti-Spoofing for L2/L3 Access Interfaces and Filter configuration.
aosqos	AoS QoS - Quality of Service for Application over Signaling (AoS QoS) Policy and conditions, AoS QoS configuration for Physical Port and Layer 2 Bridge.
aossas	AOS SAS - OAM tests specific to AOS nodes.
aossas.CPETestGroupHead	CPE SLA Test Group - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
aossas.CPETestHead	CPE SLA Test - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.

(1 of 20)

Package.Class.Method/Property	Description
apipe	APipe - All contained objects are listed. Package access is not currently used.
apipe.Apipe	Apipe Service - Access to VLL ATM Pipe (Apipe) Service objects themselves.
apipe.Site	Apipe Site - Access to Apipe Sites.
aps	APS - Automatic Protection Switching (APS) Groups.
arp	ARP - ARP host and configurations on service interfaces.
atm	ATM - ATM configuration for Service interfaces and routers, ATM Connections, ILMI Link, and other ATM related objects.
atm.AtmPing	ATM Ping - Access to ATM Ping tests, ATM Ping test definitions, and ATM Ping deployed tests.
atmpolicy	ATM QoS Policy - ATM Traffic Descriptor Policy.
audit	Resource Audit - Ability to execute audits and view audit results.
autoconfig	Automatic Configuration - Auto-Config Source and Target Node Profiles.
autoconfig.AutoConfigScriptManager.method_config ure	Automatic Configuration - method_configure - Ability to create/modify/delete an auto-config script.
autoconfig.AutoConfigScriptManager.method_copyC ontents	Automatic Configuration - method_copyContents - Ability to copy the contents of one auto-config script to new one.
bfd	BFD - Bi-Directional Forwarding Detection (BFD) can be configured on rtr.NetworkInterface, ies.L3AccessInterface, vprn.L3AccessInterface and vprn.NetworkInterface.
bgp	Routing Management: BGP - Border Gateway Protocol (BGP) configuriation for routers, policies, peers, groups, MD5, and Confederations.
bgp.Site	BGP Site - Access to a BGP protocol site on a router.
bulk	Bulk Operations - Not currently used.
bulk.BulkChange	Bulk Change - The abilty to create, modify, and/or delete bulk changes.
bulk.BulkManager.method_execute	Bulk Operations Manager - method_execute - The ability to execute bulk operations.
bulk.BulkManager.method_generateBatches	Bulk Operations Manager - method_generateBatches - The ability to generate batches for bulk operations.
bundle	Bundle - Bundle configuration for T1/E1 Multilink Group and channel members, APS, Multichassis and Service interfaces.
cac	CAC - CAC configuration for Physical Links, Physical Port and other CAC related objects.
ccag	CCAG - Cross-Connect Aggregation Group (CCAG) MDA card and forwarding path configuration.
cflowd	Cflowd - CFLOWD Objects.
cflowd.NeCflowd	Cflowd Configuration - Ability to configure cflowd params for SR.
cflowd.NeCollector	Cflowd Collector Configuration - Ability to configure collector for cflowd params for SR.
circem	CES - Configuration of Circuit Emulation Service (CES) properties for circuits and daughter cards.

(2 of 20)

Package.Class.Method/Property	Description
clear	Clear - Clear application commands and requests.
cli	CLI - Ability to connect to open NE sessions from SAM.
cli.SSH	Cli. SSH - Ability to open an SSH Telnet session to the node from SAM.
cli.Telnet	Cli. Telnet - Ability to open a Telnet session to the node from SAM.
connprof	Connection Profile - Connection Profile configuration.
cpipe	CPipe - Access to this package is for configuring CES Interface Specifics for Cpipe specific SAPs.
cpipe.Cpipe	Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
cpipe.Site	Cpipe Site - Access to Cpipe Sites.
crdtctrl	Credit Control - Credit Control configuration.
customproperties	Custom Properties - Custom properties configuration.
db	Database - Configuration for Size contraint policies and Database file policies.
db.DatabaseManager.method_backup	Database Manager - method_backup - Ability to perform a database backup.
db.DatabaseManager.method_reinstantiateStandby	Database Manager - method_reinstantiateStandby - Ability to re-instantiate the standby database.
db.DatabaseManager.method_switchover	Database Manager - method_switchover - Ability to perform a database switchover.
dhcp	DHCP - Dynamic Host Configuration Protocol (DHCP) Server for rtr.VirtualRouter and vprn.Site.
diameter	Diameter - Access to this package is for configuring Diameter related configurations, e.g. Diameter Policy.
epipe	EPipe - Access to this package is for configuring CES Interface Specifics and FR Interface Specifics for Epipe specific SAPs.
epipe.Epipe	Epipe Service - Access to VLL Ethernet Pipe (Epipe) Service objects themselves.
epipe.PbbMacName	PBB MAC Name - Ability to configure the MAC Name Address for a Network Element.
epipe.Site	Epipe Site - Access to Epipe Sites.
equipment	Physical Equipment - General equipment configuration.
ethernetequipment	Ethernet Equipment - Ethernet Equipment configuration.
ethernetoam	Ethernet OAM - Maintenance Domains and Maintenance Entity Groups, autogeneration of the MEPs on each SAP or Binding in a Service.
ethernetoam.CcmTest	CFM Continuity Check - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CcTest	Global Maintenance Entity Group - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CfmEthTest	CFM Eth Test - Access to CFM EthTests, CFM EthTest definitions, and CFM EthTest deployed tests.

(3 of 20)

Package.Class.Method/Property	Description
ethernetoam.CfmLinkTrace	CFM Link Trace - Access to Link Trace tests, Link Trace test definitions, and Link Trace deployed tests.
ethernetoam.CfmLoopback	CFM Loopback - Access to CFM Loopback tests, CFM Loopback test definitions, and CFM Loopback deployed tests.
ethernetoam.CfmOneWayDelayTest	CFM One Way Delay Test - Access to CFM One Way Delay tests, CFM One Way Delay test definitions, and CFM One Way Delay deployed tests.
ethernetoam.CfmOneWaySlm	CFM One Way SLM Test - Access to CFM One Way SLM tests, CFM One Way SLM test definitions, and CFM One Way SLM deployed tests.
ethernetoam.CfmSingleEndedLossTest	CFM Single Ended Loss Test - Access to CFM Single Ended Loss tests, CFM Single Ended Loss test definitions, and CFM Single Ended Loss deployed tests.
ethernetoam.CfmTwoWayDelayTest	CFM Two Way Delay Test - Access to CFM Two Way Delay tests, CFM Two Way Delay test definitions, and CFM Two Way Delay deployed tests.
ethernetoam.CfmTwoWaySlm	CFM Two Way SLM Test - Access to CFM Two Way SLM tests, CFM Two Way SLM test definitions, and CFM Two Way SLM deployed tests.
ethernetservice	Ethernet Service Policy - SAP Profile and UNI Profile policies.
ethernettunnel	Ethernet Tunnel - Ethernet Tunnel configuration.
ethring	Ethernet Ring - Ethernet Ring Configuration.
fabricqos	Fabric QoS Policies - Fabric Profile QoS policy.
file	File Policy - File creation on the NE for events and accounting.
filter	Filter - Public search filters.
fm	Fault Management - Alarm policies, Severity change thresholds, Alarms, Notes, and History.
fm.AlarmHistoryDatabase.method_purge	Alarm History Database - method_purge - Ability to purge the alarm history database.
fm.FaultManager	Fault Manager - Access to assign OLC state, alter severity, clear, acknowledge, and remove faults.
fm.FaultManager.method_editNote	Fault Manager - method_editNote - Ability to edit an alarm note.
fm.GlobalPolicy	Global Alarm Behavior - Access to configure the global alarm behavior.
fm.SpecificPolicy	Specific Alarm Policy - Access to configure specific alarm policies.
fpipe	FPipe - All contained objects are listed. Package access is not currently used.
fpipe.Fpipe	Fpipe Service - Access to Frame Relay Pipe (Fpipe) Service objects themselves.
fpipe.Site	Fpipe Site - Access to Fpipe Sites.
fr	Frame Relay - Frame Relay configuration for Service interfaces and routers.
generic	Generic - Generic configuration for SAM objects, deployment, and administrative state changes for DHCP and Multichassis objects, Maintenance Association End Points (MEP), and SRRP instances.

(4 of 20)

Package.Class.Method/Property	Description
generic.GenericObject.method_collectData	GenericObject - method_collectData - Ability to collect and plot real-time statistics.
genericne	Generic NE - Generic NE Interface and Profile configuration.
gsmp	GSMP - General Switch Management Protocol (GSMP) configuration for VPLS, MVPLS and VPRN routing instances.
hip	Horizontal Integration Protocol - Access to HIP managed Element Managers and subtending nodes.
hip.EMServer	Element Manager - Access to HIP managed Element Managers.
hip.EMSystem	EM System - Access to HIP managed EM Systems.
hpipe	HPipe - All contained objects are listed. Package access is not currently used.
hpipe.Hpipe	Hpipe Service - Access to HPipe (Hpipe) Service objects themselves.
hpipe.Site	Hpipe Site - Access to Hpipe Sites.
icmp	ICMP - Internet Control Message Protocol (ICMP) and Domain Name System (DNS) test results.
icmp.DnsPing	DNS Ping - Access to DNS Ping tests, DNS Ping test definitions, and DNS Ping deployed tests.
icmp.IcmpPing	ICMP Ping - Access to ICMP Ping tests, ICMP Ping test definitions, and ICMP Ping deployed tests.
icmp.IcmpTrace	ICMP Trace - Access to ICMP Trace tests, ICMP Trace test definitions, and ICMP Trace deployed tests.
ies	IES - Access to this package is for configuring Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for IES specific SAPs.
ies.Ies	IES Service - Access to Internet Enhanced Service (IES) Service objects themselves.
ies.L3AccessInterface	IES L3 Access Interface - Access to IES L3 Access Interfaces.
ies.Site	IES Site - Access to IES Sites.
ies.SubscriberInterface	IES Subscriber Interface - Access to IES Subscriber Interfaces.
igh	IGH - Interface-Group-Handlers.
igmp	IGMP - Internet Group Management Protocol (IGMP) configuration for Service interfaces and routers.
igmp.Site	IGMP Site - Access to IGMP Sites.
impact.FullReset	Impact. Full Reset - Ability to configure objects which will result in a full reset of the node. Currently applies to 9412 node.
impact.PartialReset	Impact. Partial Reset - Ability to configure objects which will result in a partial reset of impacted SW/HW unit. Currently applies to 9412 node.
ipipe	IPipe - Access to this package is for configuring IPCP on L2 Access Interfaces and FR Interface Specifics for Ipipe specific SAPs.
ipipe.Ipipe	Ipipe Service - Access to IP Interworking Pipe (Ipipe) Service objects themselves.
ipipe.L2AccessInterface	IPipe L2 Access Interface - Access to IPipe L2 Access Interfaces.
ipipe.Site	Ipipe Site - Access to Ipipe Sites.

(5 of 20)

Package.Class.Method/Property	Description
ipsec	IP Security - IKE Policy and IPsec Transform.
isa	ISA - ISA-IPsec, ISA-MG, and ISA-AA configuration on a MDA card for IP Security, LTE, and Application Assurance.
isa.MgGroupMember	ISA-MG Group Member - Configuration of ISA-MG Group Member.
isa.MgIsaGroup	ISA-MG Group - Configuration of ISA-MG Group.
isis	Routing Management: ISIS - IS-IS configuration for Service interfaces and routers, Area, Adjacency, Neighbors, Policies and other IS-IS related objects.
l2fib	L2 FIB - Layer 2 Forwarding Information Base (FIB) configuration for Multicast and Non-Multicast.
l2fwd	L2 Forwarding - All Layer 2 Forwarding configuration for Service interfaces and routers, ciruits, ports, Spanning Tree, Registration, FIB, Mac Protection, IGMP Snooping, etc.
l2tp	L2TP - L2TP configuration for Service interfaces and routers, Groups, Tunnels, PeersRPs, and other L2TP related objects.
l3fwd	L3 Forwarding - All Layer 3 Forwarding configuration for Service interfaces and routers, Import and Export policies, Dot1p and DSCP for VPRNs.
lag	LAG - Link Aggregation Group (LAG) configuration for Service interfaces and routers.
layer2	Layer 2 - All Layer 2 configuration: Bridges, Transparent LAN Service (TLS), and VLAN interfaces.
ldp	Routing Management: LDP - Label Distribution Protocol (LDP) configuration for Service interfaces and routers, Session, MD5 Key, Equal-Cost Multipath Routing (EMCP), Forwarding Equivalency Class (FEC), Policies, and Peers.
lldp	LLDP - Link Layer Discovery Protocol (LLDP) configuration on equipment.PhysicalPort.
localuserdb	Local User DB - DHCP or PPPoE configuration for Local User Databases on a router.
log	Statistics - Parent package for all statistics classes.
log.LogToFileManager.property_retention	LogToFileManager - property_retention - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_rollover	LogToFileManager - property_rollover - LogToFile preferences can only be modified by a user with an administrator role.
lps	LPS - Learned Port Security (LPS) configuration for layer2.Bridge and MAC Entries for ports.
lte	LTE - All LTE configurations and status.
lte.CallTraceDirectory	Call Trace Directory - Configuration of Call Trace Directory.
lte.DccaProfile	DCCA Profile - Configuration of DCCA Profile.
lte.DiameterPeerListEntry	Diameter Peer List Entry - Configuration of Diameter Peer List Entry.
lte.DiameterPeerProfile	Diameter Peer Profile - Configuration of Diameter Peer Profile.
lte.DiameterProfile	Diameter Profile - Configuration of Diameter Profile.
lte.DiscoveryLog	Drill Down Log - Creation of Drill Down Log.

(6 of 20)

Package.Class.Method/Property	Description
lte.DupRadiusAccServerGroup	Duplicate Accounting RADIUS Server Group - Configuration of Serving Gateway APN.
lte.ENBEquipment.method_launchNEM	ENB Equipment - method_launchNEM - Ability to launch NEM.
lte.EPSPathDiscoveredLinkComponent	EPS Path Discovery Link Component - Configuration of EPS Path Discovery Link Component.
lte.EPSPathDiscoveryHint	EPS Path Drill Down Hint - Configuration of EPS Path Drill Down Hint.
lte.EPSPathDiscoveryProfile	Path Drill Down Profile - Configuration of Path Drill Down Profile.
lte.EPSPathInterfaceComponent	EPS Path Interface Component - Configuration of EPS Path Interface Component.
lte.EPSPathLinkComponent	EPS Path Link Component - Configuration of EPS Path Link Component.
lte.EPSPathSapComponent	EPS SAP Component - Configuration of EPS SAP Component.
lte.EPSPathSegment	EPS Path Segment - Configuration of EPS Path Segment.
lte.EPSPathServiceComponent	EPS Path Service Component - Configuration of EPS Path Service Component.
lte.EPSPathSiteComponent	EPS Path Site Component - Configuration of EPS Path Site Component.
lte.GtpPrimaryServerListEntry	GTP Primary Server List Entry - Configuration of GTP Primary Server List Entry.
lte.GtpPrimeServerGroupProfile	GTP Prime Server Group Profile - Configuration of GTP Prime Server Group Profile.
lte.GtpProfile	GTP Profile - Configuration of GTP Profile.
lte.IpPool	IP Address Pool - Configuration of IP Address Pool.
lte.IpPoolBinding	IP Address Pool Binding - Configuration of IP Address Pool Binding.
lte.IpPoolEntry	IP Address Pool Entry - Configuration of IP Address Pool Entry.
lte.MobileNodeRegion	Mobile Node Region/Public Land Mobile Network (PLMN) - Configuration of Mobile Node Region.
lte.PdnApn	PDN APN - Configuration of PDN APN.
lte.PDNGateway	PDN Gateway - Configuration of PDN Gateway.
lte.PdnGxReferencePoint	PDN Gx Reference Point - Configuration of Pdn Gx Reference Point.
lte.PdnS5ReferencePoint	PDN S5 Reference Point - Configuration of PGW S5 Reference Point.
lte.PdnS8ReferencePoint	PDN S8 Reference Point - Configuration of PGW S8 Reference Point.
lte.PdnSignalling	PGW Signalling - Configuration of PGW Signalling.
lte.PgwChargingProfile	PGW Charging Profile - Configuration of PGW Charging Profile.
lte.PlmnListPolicy	PLMN List Profile - Configuration of PLMN List Profile.
lte.PlmnListPolicyGroup	PLMN List Group - Configuration of PLMN List Group.
lte.QciPolicy	QCI Policy - Configuration of QCI Policy.
lte.QciPolicyEntry	QCI Policy Entry - Configuration of QCI Policy Entry.
lte.S11ReferencePoint	S11 Reference Point - Configuration of S11 Reference Point.
lte.S1uReferencePoint	S1-u Reference Point - Configuration of S1u Reference Point.

(7 of 20)

Package.Class.Method/Property	Description
lte.ServingGateway	Serving Gateway - Configuration of Serving Gateway.
lte.SgwApn	Serving Gateway APN - Configuration of Serving Gateway APN.
lte.SgwChargingProfile	SGW Charging Profile - Configuration of SGW Charging Profile.
lte.SgwRfReferencePoint	SGW Rf - Configuration of SGW Rf Reference Point.
lte.SgwS5ReferencePoint	SGW S5 Reference Point - Configuration of SGW S5 Reference Point.
lte.SgwS8ReferencePoint	SGW S8 Reference Point - Configuration of SGW S8 Reference Point.
lte.SgwSignalling	Serving Gateway Signalling - Configuration of Serving Gateway Signalling.
lte.SubscAndEquipmentTraces	Subsc And Equipment Traces - Configuration of Call Traces.
lte.TrustedPeerListEntry	Trusted Peers - Configuration of Trusted Peer List Entries.
lte.TrustedPeerListEntryUnlisted	Unlisted Peer - Configuration of Unlisted Trusted Peer List Entries.
lte.TrustedPeerListPolicy	Trusted Peer List Policy - Configuration of Trusted Peer List Policy.
lteanr	LTE - Access to LTE ANR profiles.
lteggsn	LTE - All LTE configurations and status.
lteggsn.GnReferencePoint	Gn Reference Point - Configuration of Gn Reference Point.
lteggsn.PdnGyReferencePoint	Gy Reference Point - Configuration of Gy Reference Point.
lteggsn.PgwGaReferencePoint	PGW Ga Reference Point - Configuration of PGW Ga Reference Point.
lteggsn.SgwGaReferencePoint	SGW Ga Reference Point - Configuration of SGW Ga Reference Point.
lteli	LTE LI - All LTE LI configurations and status.
lteli.DFPeer	LTE LI Delivery Function Peer - Configuration of LTE LI Delivery Function Peer.
lteli.InterceptionTarget	LTE LI Interception Target - Configuration of LTE LI Interception Target.
ltemme	LTE - All LTE MME configurations.
ltemme.MmeInstance.method_abortMmeLoadBalance	MME Instance - method_abortMmeLoadBalance - Ability to abort MME load balancing operation.
ltemme.MmeInstance.method_interMmeLoadBalance	MME Instance - method_interMmeLoadBalance - Ability to perform inter MME load balancing operation.
ltemme.MmeInstance.method_intraMmeLoadBalance	MME Instance - method_intraMmeLoadBalance - Ability to perform intra MME load balancing operation.
ltemme.MmeInstance.method_lockMmeAggregateService	MME Instance - method_lockMmeAggregateService - Ability to lock the MME aggregate service.
ltemme.MmeInstance.method_unlockMmeAggregateService	MME Instance - method_unlockMmeAggregateService - Ability to unlock the MME aggregate service.
lteperf	LTE Performance Management - All LTE configurations : SGW, PGW, eNodeB.
ltepmip	LTE - All LTE configurations and status.
ltepmip.Pmipv6Profile	PMIPv6 Profile - Configuration of PMIPv6 Profile.

(8 of 20)

Package.Class.Method/Property	Description
ltepmip.S2aReferencePoint	S2a Reference Point - Configuration of S2a Reference Point.
ltepool	LTEPOOL - All LTE POOL configurations.
ltepool.MmeInstanceBinding	MME Instance Binding - Ability to configure associations between an MME Instance and an MME Pool.
ltepool.TaBinding	Tracking Area Binding - Ability to configure associations between a Tracking Area and an MME Pool.
lteradius	LTE - All LTE configurations and status.
lteradius.RadiusGroupProfile	RADIUS Group Profile - Configuration of Radius Group Profile.
lteradius.RadiusPeerProfile	RADIUS Peer Profile - Configuration of RADIUS Peer Profile.
lteradius.RadiusProfile	RADIUS Profile - Configuration of RADIUS Profile.
ltes1mme	LTES1MME - All LTE S1MME Configurations and Monitoring Status.
ltesecurity	LTE Security - All LTE configurations : SGW, PGW, Bearers, and more.
lteservice	LTE - All LTE configurations and status.
ltethreshold	LTE - All LTE configurations and status.
lteuserstats	LTE - All LTE configurations and status.
lteuserstats.UserStatsQuery	User Stat Query - Configuration of User Stats Queries.
lteuserstats.UserStatsQueryOutputSnapshot	User Query Output Snapshot - Configuration of User Stats Query Snapshots.
lteuserstats.UserStatsUserPgw	PGW User Data - Configuration of User Stats User Output.
lteuserstats.UserStatsUserSgw	SGW User Data - Configuration of User Stats User Output.
mediation	Router Admin: Policies - Router administration: Backup Policies, Upgrade Policies and Software images, Deployment Policies, and Management Ping Policies.
mirror	Mirror - All configurations for Service Mirroring.
mirror.Endpoint	Endpoint - Access to MIRROR Endpoints.
mirror.Mirror	Mirror Service - Access to Mirror Service objects themselves.
mirror.Site	Mirror Site - Access to Mirror Sites.
mld	MLD - Multicast Listener Discovery Protocol (MLD) configuration for a Service interfaces and routers.
mmepolicy	mmepolicy.
mmepolicy.MMEGTPProfile	MME GTP Profile - Configuration of GTP Profile.
mmepolicy.MMESCTPProfile	MME SCTP Profile - Configuration of SCTP Profile.
monitor	Monitor - Subscriber Host monitoring and SAP monitoring.
monpath	Monitored Path - IP path monitoring and LSP monitoring.
mpls	Path/Routing Management: MPLS - Multiprotocol Label Switching (MPLS) configuration on a rtr.VirtualRouter, LSPs, Segments, Hops, Tunnels, CrossConnects, and other MPLS related objects.
mpls.LdpTreeTrace	LDP Tree Trace - Access to LDP Tree Trace tests, LDP Tree Trace test definitions, and LDP Tree Trace deployed tests.
mpls.LspPing	LSP Ping - Access to LSP Ping tests, LSP Ping test definitions, and LSP Ping deployed tests.

(9 of 20)

Package.Class.Method/Property	Description
mpls.LspTrace	LSP Trace - Access to LSP Trace tests, LSP Trace test definitions, and LSP Trace deployed tests.
mpls.P2MPLspPing	P2MP LSP Ping - Access to P2MP LSP Ping tests, P2MP LSP Ping test definitions, and P2MP LSP Ping deployed tests.
mpls.P2MPLspTrace	P2MP LSP Trace - Access to P2MP LSP Trace tests, P2MP LSP Trace test definitions, and P2MP LSP Trace deployed tests.
mpr	9500 MPR - 9500 Microwave Packet Radio (MPR) VLAN Paths and Hops.
mpr.Al2AccessInterface	L2 Access Interface - Access to L2AccessInterface objects.
mpr.Apipe	9500 MPR Apipe Service - Access to vll ATM Pipe (Apipe) Service objects themselves.
mpr.Asite	Apipe Site - Access to the service instance objects.
mpr.Cpipe	9500 MPR Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
mpr.El2AccessInterface	L2 Access Interface - Access to L2AccessInterface objects.
mpr.Epipe	9500 MPR Epipe Service - Access to VLL Ethernet Pipe Service objects themselves.
mpr.Esite	Epipe Site - Access to the service instance objects.
mpr.L2AccessInterface	L2 Access Interface - Access to L2AccessInterface objects.
mpr.Site	Cpipe Site - Access to the service instance objects.
msappolicy	MSAP Policy - MSAP policy configuration.
msdp	MSDP - Multicast Source Discovery Protocol (MSDP) configuration for a rtr.VirtualRouter, MD5 Key, Peers, Policies and Source.
multicast	Multicast - Multicast Connection Admission Control (CAC) Policies and Bandwidth Policies.
multicast.CustomerVlanTag	Customer Vlan Tag - Configuration of Customer VLAN Tags for a Multicast VLAN.
multicast.MfibPing	MFIB Ping - Access to MFIB Ping tests, MFIB Ping test definitions, and MFIB Ping deployed tests.
multicast.Mrinfo	Mrinfo - Access to Mrinfo tests, Mrinfo test definitions, and Mrinfo deployed tests.
multicast.Mtrace	Mtrace - Access to Mtrace tests, Mtrace test definitions, and Mtrace deployed tests.
multicastmgr	CPAM: Multicast - All CPAM Multicast related objects: PIM Domain, VPLS Domain, Groups, and Sources.
multichassis	Multi-Chassis - Multi-Chassis configuration for a router; LAGs, Rings, Syncs, Peers, VLAN Ranges.
mvpls	MVPLS - All contained objects are listed. Package access is not currently used.
mvpls.BL2AccessInterface	MVPLS B-L2 Access Interface - Access to MVPLS B-L2 Access Interfaces.
mvpls.BSite	MVPLS B-Site - Access to MVPLS B-Sites.
mvpls.IL2AccessInterface	MVPLS I-L2 Access Interface - Access to MVPLS I-L2 Access Interfaces.
mvpls.ISite	MVPLS I-Site - Access to MVPLS I-Sites.

(10 of 20)

Package.Class.Method/Property	Description
mvpls.L2AccessInterface	MVPLS L2 Access Interface - Access to MVPLS L2 Access Interfaces (except I and B).
mvpls.Mvpls	MVPLS Service - Access to Management Virtual Private LAN Service (MVPLS) Service objects themselves.
mvpls.Site	MVPLS Site - Access to MVPLS Sites (except I and B).
mvrp	MVRP - MVRP global configuration and for Interfaces(Ports and LAG's).
nat	Network Address Translation - NAT Policy.
netca	NE Threshold Crossing Alerts - Manage NE Threshold Crossing Alert profiles.
netw	Network - Network objects: groups and links.
netw.NetworkElement	Network Element - Access to Network Elements.
netw.NetworkElement.method_executeCli	Network Element - method_executeCli - Execute a single raw CLI command on this Network Element.
netw.NetworkElement.method_executeMultiCli	Network Element - method_executeMultiCli - Execute Multiple CLI commands on this Network Element.
netw.NetworkElement.method_GUICrossLaunch	Network Element - method_GUICrossLaunch - The ability to launch LTE web-browser based tools.
netw.NodeDiscoveryControl	Node Discovery Control - Control of Discovered Nodes.
netw.Topology	Discovery Manager - Access to the Discovery Manager.
netw.Topology.method_move	Discovery Manager - method_move - Ability to move a node or group on the SAM Client GUI maps.
netw.UplinkBofConfiguration	Uplink Bof Configuration - Ability to configure the Uplink BOF for a 7210 node.
netw.UplinkRouteConfiguration	Uplink Route Configuration - Ability to configure the Uplink Routes for a 7210 node.
niegr	Network Ingress/Egress Policy - Network Policies.
nodelog	Node Log Policy - Filter Log and Sys Log Target Policies.
nqueue	Network Queue Policy - Network Queue QoS Policies.
ntp	Network Time Protocol - Network Time Protocol.
optical	Optical Specifics - Optical NE Specific Information.
optical.DiverseService	Diverse Optical Transport Service - Access for all optical services.
optical.SubRateService	SubRate Optical Transport Service - Access for all optical services.
optical.TransportService	Optical Transport Service - Access for all optical services.
optical.YCableService	Diverse Optical Transport Service - Access for all optical services.
opticsperf	Optics Specifics - All 1830 PSS configurations.
ospf	Routing Management: OSPF - OSPF configuration for Service interfaces and routers, Area, Adjacency, MD5 Key, Virtual Links Neighbors, LSAs, Policies and other OSPF related objects.
ospf.Site	OSPF Site - Access to OSPF Sites.
oss	OSS - Ability to connect to the SAM Server through the OSS interface.

(11 of 20)

Package.Class.Method/Property	Description
pae802_1x	PAE 802.1x - Port Access Entity (PAE) configuration for a router and physical port; RADIUS Server Policy.
pim	PIM - PIM configuration for Service interfaces and routers, MDT Threshold, Policies, Neighbors, Groups, RPs, Multicast CAC Level and LAG Port Down events, and other PIM related objects.
pim.Site	PIM Site - Access to PIM Sites.
policing	Policing Policy - Policer Control.
policy	Policy - Parent package for all policies; Policy Audits.
policy.PolicyDefinition.method_setConfigurationModeToReleased	Policy Definition - method_setConfigurationModeToReleased - Ability set Configuration Mode to Released and distribute the global policy to the local definitions network-wide.
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Policy Definition - method_setDistributionModeToLocalEditOnly - Ability set Configuration Mode to Local Edit Only for local policies and ignore changes to the global policy.
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Policy Definition - method_setDistributionModeToSyncWithGlobal - Ability set Configuration Mode to Sync with Global and synchronize local policies with the most recent released global policy.
policy.PolicySyncGroupManager	Policy Sync Group Manager - Ability to configure and control policy sync group.
port.RestrictModeConfigModify	Port. Restrict Mode Config Modify - Ability to restrict Port Mode modification for Ports with dependencies.
portscheduler	Port Scheduler Policy - Port Scheduler and HSMDA Scheduler Policies.
ppp	PPP - Point-to-Point Protocol (PPP) configuration on a router.
pppoe	PPP Policy and Session - Point-to-Point Protocol over Ethernet over ATM (PPPoE/PPPoEoA/PPPoA) Policies and Sessions.
propertyrules	Property Rules - Range and Format Value Policies.
ptp	ptp.
qgroup	Queue Group Policy - Queue Group Policies.
qosprofile	Multilink QoS Profile - Multilink PPP QoS Profiles and Multilink Frame Relay QoS Profiles.
radioequipment	Radio Equipment - Radio Equipment configuration.
radiusaccounting	Radius Accounting - Radius Accounting Policy.
ranlicense	NE License Management - Ability to manage NE licenses.
ranradiom	eNodeB Router Admin: radio measurement - eNodeB Router administration: radio measurement.
rca	RCA - Root Cause Analysis (RCA) for verification applications (OSPF Area,ISIS Area,BGP AS,...).
rca.RcaManager.method_fixProblem	RcaManager - method_fixProblem - Ability to fix a problem on an object.
rca.RcaManager.method_preFixProblem	RcaManager - method_preFixProblem - Ability to determine if a problem can be fixed, and the fix impact.
resiliency	HSDPA Resiliency - HSDPA Resiliency for services.
resources	SAM Resources - SAM Resource Pools as configured in the nms-server.xml file.

(12 of 20)

Package.Class.Method/Property	Description
ressubscr	Residential Subscriber - All Residential Subscriber configuation including Connectivity Verifications (SHCV), SAPs, Packages, Hosts, QoS, and other related objects.
ressubscr.BgpPeeringPolicy	BGP Peering Policy - Access to BGP Peering Policies.
ressubscr.HostTrackingPolicy	Host Tracking Policy - Access to Host Tracking Policies.
ressubscr.IgmpPolicy	IGMP Policy - Access to IGMP Policies.
ressubscr.SubMcastCacPolicy	Subscriber Multicast CAC Policy - Access to Subscriber Multicast CAC Policies.
rip	Routing Management: RIP - Routing Information Protocol (RIP) configuration for Service interfaces and routers, Authentication Key, Groups, Export and Import Policies.
rip.Site	RIP Site - Access to RIP Sites.
rmon	Remote Network Monitoring - Remote Network Monitoring Alarm and Event Policies.
rp	Routing Policy - Policy Statements, Prefix Lists, Communities, Damping, and AS Paths.
rsvp	Routing Management: RSVP - RSVP configuration for a rtr.VirtualRouter, Authentication Keys, and Neighbors.
rtr	Routing Management: General - General rtr.VirtualRouter configurations including Neighbor Discovery, DHCP Relays, Interfaces, Peers, Address Ranges and ARP, Routes and Router Advertisement.
rules	Rules - Rule Repository and Sets of rules that may get invoked when a rule engine is fired.
sas	Assurance - Parent package for all tests; Service Test Manager.
sas.TestManager.property_sasRetention	Service Test Manager - property_sasRetention - LogToFile preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRollover	Service Test Manager - property_sasRollover - LogToFile preferences can only be modified by a user with an administrator role.
sasqos	7210 QoS - QoS Policies for 7210 nodes.
sasqos.QosPool	QoS Pool - Access to QoS Pools for 7210 nodes.
schedule	Schedule - All scheduled tasks; Cron Actions, OSS Commands, CLI Scripts and Schedules.
script	Scripting - Script Management and execution of Service and Tunnel Template, OSS, and CLI scripts.
script.AbstractScript.method_configureTarget	Script - method_configureTarget - Ability to configure targets and instances.
script.AbstractScript.method_configureTargets	Script - method_configureTargets - Ability to configure targets and instances.
script.Bundle	Script Bundle - Ability to configure script bundles.
script.ControlScript	Control Script - Ability to configure control scripts.
script.ControlScriptVersion	Control Script Version - Ability to configure Control script versions.
script.HandlerBinding	Handler Script Binding - Ability to configure associations between scripts and control scripts.

(13 of 20)

Package.Class.Method/Property	Description
script.InvokerBinding	Invoker Script Binding - Ability to configure associations between scripts and control scripts.
script.LargeTextTargetParameter	Large Text Target Parameter - Ability to configure target/instance large text parameters.
script.Result	Result - Ability to create script results.
script.Script	CLI Script - Ability to configure CLI scripts.
script.Script.method_createTargetScript	CLI Script - method_createTargetScript - Ability to configure targets.
script.Script.method_createTargetScripts	CLI Script - method_createTargetScripts - Ability to configure targets.
script.ScriptManager	Script Manager - Ability to configure and control scripts and script operations.
script.ScriptManager.method_configure	Script Manager - method_configure - Ability to configure scripts.
script.ScriptManager.method_copyContents	Script Manager - method_copyContents - Ability to copy scripts.
script.ScriptManager.method_exportBundle	Script Manager - method_exportBundle - Ability to export bundle.
script.ScriptManager.method_importBundle	Script Manager - method_importBundle - Ability to import bundle.
script.ScriptManager.method_importBundleSimulation	Script Manager - method_importBundleSimulation - Ability to import bundle.
script.ScriptScheduledTask	Script Scheduled Task - Ability to schedule a script.
script.TargetParameter	Target Parameter - Ability to configure target/instance parameters.
script.TargetParameterItem	Target Parameter Item - Ability to configure target/instance parameter items.
script.TargetParameterList	Target Parameter List - Ability to configure target/instance parameter lists.
script.TargetScript	Target Script - Ability to configure targets and instances.
script.TemplateBinding	Template Binding - Ability to configure associations between templates.
script.Version	Version - Ability to configure CLI script versions.
script.XmlApiConfigTemplate	Template - Ability to configure XML API templates.
script.XmlApiConfigTemplate.method_execute	Template - method_execute - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeMulti	Template - method_executeMulti - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeScript	Template - method_executeScript - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Template - method_serviceTemplateExecute - Ability to execute a service template.
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Template - method_tunnelTemplateExecute - Ability to execute a tunnel template.
script.XmlApiScript	XMLAPI Script - Ability to configure XML API scripts.
script.XmlApiVersion	XMLAPI Version - Ability to configure XML API script versions.
security	Security - SAM User security including Sessions, TCP KeyChains, and SSH2 Known Host Keys.

(14 of 20)

Package.Class.Method/Property	Description
security.CpamLicense	CPAM License - Read-only view of the 5650 CPAM License.
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	CPAM License - method_clearRouterLimitExceedDueToMultiAdditions - Ability to clear the isRouterLimitExceedDueToMultiAdditions flag on the license.
security.CpamLicenseScenario	CPAM License Scenario - Read-only view of the 5650 CPAM Imapct Analysis Application License.
security.MediationPolicy	Mediation Policy - Access to Mediation Policies. Used in conjunction with snmp.PollerManager.
security.MessagingConnection	Messaging Connection - Ability to view messaging connections.
security.RoleBasedAccess	Security. Role Based Access - Ability to restrict online object creation and deletion to a specific role. Currently applies to 9412 node.
security.ScopeOfCommandProfile	Profile - Access to Scope of Command Profile configuration.
security.ScopeOfCommandRole	Role - Access to Scope of Command Role configuration.
security.Span	Span - Access to Span configuration. Used in conjunction with security.SpanObjectBinding.
security.SpanObjectBinding	Span Objects - Access to Span object configuration. Used in conjunction with security.Span.
security.SpanOfControlProfile	Profile - Access to Span of Control Profile configuration.
security.User	User - Access to User object configuration and password changes.
security.UserGroup	UserGroup - Access to UserGroup configuration.
selfconfig	Self Config - Ability to configure self config objects.
server	SAM Server - SAM Servers (JMS, Main, Auxilary) as configured in the nms-server.xml file.
service	Service Management - Parent package for all services; Composite Services and Connectors and Access Policy Queue Override Policies.
service.CpePing	CPE Ping - Access to CPE Ping tests, CPE Ping test definitions, and CPE Ping deployed tests.
service.GneAccessInterface	GNE Service Interface - Access to GNE Service Interfaces.
service.GneSite	GNE Site - Access to GNE Sites.
service.MacPing	MAC Ping - Access to MAC Ping tests, MAC Ping test definitions, and MAC Ping deployed tests.
service.MacPopulate	MAC Populate - Access to MAC Populate tests, MAC Populate test definitions, and MAC Populate deployed tests.
service.MacPurge	MAC Purge - Access to MAC Purge tests, MAC Purge test definitions, and MAC Purge deployed tests.
service.MacTrace	MAC Trace - Access to MAC Trace tests, MAC Trace test definitions, and MAC Trace deployed tests.
service.MefMacPing	MEF MAC Ping - Access to MEF MAC Ping tests, MEF MAC Ping test definitions, and MEF MAC Ping deployed tests.
service.RedundantInterface	Redundant Interface - Access to Redundant Interface configuration between SRRP instances.

(15 of 20)

Package.Class.Method/Property	Description
service.Service.method_create	Service - method_create - Ability to create a service via the SAM Client GUI.
service.Service.method_highPriorityServiceDelete	Service - method_highPriorityServiceDelete - Ability to delete high priority Service.
service.Service.property_svcPriority	Service - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceManager.property_alarmAggregationCompositeService	ServiceManager - property_alarmAggregationCompositeService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_autoDiscoverCompositeSvc	ServiceManager - property_autoDiscoverCompositeSvc - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableCac	ServiceManager - property_enableCac - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_maxNumberOfMoveSites	ServiceManager - property_maxNumberOfMoveSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_multiSegmentTunnelSelection	ServiceManager - property_multiSegmentTunnelSelection - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_propagateServiceNameToSites	ServiceManager - property_propagateServiceNameToSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_removeEmptyService	ServiceManager - property_removeEmptyService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_supVprnSnmpCommunityStringMsg	ServiceManager - property_supVprnSnmpCommunityStringMsg - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_svcPriority	ServiceManager - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceMemberAuditPolicyEntry	Service Membership Audit Policy Entry - Access to Service Member Audit Policy Entry to configure service membership RCA audit behavior.
service.SitePing	Service Site Ping - Access to Service Site Ping tests, Service Site Ping test definitions, and Service Site Ping deployed tests.
service.TemplateService.method_constructServiceTemplate	Service Template - method_constructServiceTemplate - Ability to construct a Template from a Service.
service.TemplateService.method_constructTemplatedService	Service Template - method_constructTemplatedService - Ability to construct a Service from a Template.
shg	Split Horizon Group - Split Horizon Groups for VPLS services.
simulator	CPAM: Simulator - Parent package for all CPAM simulated objects; Scenarios, Sessions, Change and Action events.
simulator.SimSession	Session - Access to simulation sessions for 5650 CPAM Impact Analysis.
sitesec	NE Security - All Network Element security configuration including NE System Security, RADIUS, TACACS+ and AOS Authentication, Site Management Access and CPM Filters, DoS Protection, Password Policy, Users and Profiles.

(16 of 20)

Package.Class.Method/Property	Description
sitesec.LocalUser	NE User - Access to NE Site User configuration.
sitesec.UserProfile	Site User Profile - Access to NE Site User Profile configuration.
slaprofile	SLA Profile - SLA Profiles for QoS Policies.
slope	Slope Policy - WRED Slope, HSMDA WRED Slope, HSMDA Pool, and Named Buffer Pool Policies.
slope.QosPool	QoS Pool - Access to QoS Pools for 7450, 7750, and 7710 nodes.
snmp	SNMP - SNMP Poller Policies, Event Notification Policies, Statistics Poller Policies.
snmp.EventNotificationPolicy	Event Notification Policy - Access to Event Notification Policies.
snmp.PollerManager	Mediation - Access to Mediation Policies. Used in conjunction with security.MediationPolicy.
snmp.PollerManager.method_resync	Mediation - method_resync - Ability to resync a Network Element. Requires 'update' access on netw.NetworkElement.
sonet	SONET Sync - SONET Synchronization for Shelf and Processor Cards.
sonetequipment	SONET Equipment - SONET Equipment configuration.
spanrules	Span Rules - Span Rules for service creation.
squeue	Shared Queue Policy - Shared Queue Policies.
srmrmtauth	SAM Remote Authentication - Remote Authentication for SAM configuration of RADIUS and TACACS+ authentication servers.
srrp	SRRP - Subscriber Routed Redundancy Protocol (SRRP) configuration for IES and VPRN services.
statistics	SAM Performance Statistics - SAM Performance Statistics (Memory, Alarm Rate, Snmp Traps, and Node Resyncs).
subscr	Subscriber Management - Customers configuration.
subscr.Site	Subscriber Site - Access to Subscriber Sites.
subscrauth	Subscriber Authentication - Subscriber Authentication Policy using RADIUS for DHCP sessions.
subscrexpmap	Subscriber Explicit Map - Subscriber Explict Map Entry.
subscrident	Subscriber Identification - Subscriber Identification Policy.
subscrprofile	Subscriber Profile - Subscriber Profile, SLA Entries, Access Policy Queue Overrides and Scheduler Policy Entry Overrides.
sup	Supervision - SAM Supervision (Dashboard).
svq	Aggregation Scheduler - Service and Subscriber Aggregation Scheduler, Ingress and Egress Aggregation Scheduler Overrides.
svr	Service Routing - All contained objects are listed. Package access is not currently used.
svt	Service Tunnel Management - All Service Tunnel configruations including Clouds, Service Distribution Path (SDP) Bindings and Pseudo Wires.
svt.MeshSdpBinding	Mesh SDP Binding - Access to Mesh SDP Binding configuration.
svt.MirrorSdpBinding	Mirror SDP Binding - Access to Mirror SDP Binding configuration.
svt.MtuPing	MTU Ping - Access to MTU Ping tests, MTU Ping test definitions, and MTU Ping deployed tests.

(17 of 20)

Package.Class.Method/Property	Description
svt.SpokeSdpBinding	Spoke SDP Binding - Access to Spoke SDP Binding configuration.
svt.Tunnel	Tunnel - Access to Tunnel (or SDP object) configuration.
svt.TunnelPing	Tunnel Ping - Access to Tunnel Ping tests, Tunnel Ping test definitions, and Tunnel Ping deployed tests.
svt.VccvPing	VCCV Ping - Access to VCCV Ping tests, VCCV Ping test definitions, and VCCV Ping deployed tests.
svt.VccvTrace	VCCV Trace - Access to VCCV Trace tests, VCCV Trace test definitions, and VCCV Trace deployed tests.
sw	Router Admin: Software - Router administration: Backup Files, Card Software, Upgrade schedules, and Accounting Statistics Retrieval.
sw.BackupRestoreManager.method_backup	Backup/Restore Status - method_backup - Ability to perform a Network Element backup.
sw.BackupRestoreManager.method_restore	Backup/Restore Status - method_restore - Ability to perform a Network Element restore.
swran	eNodeB Router Admin: Software - eNodeB Router administration: Upgrade schedules.
taskmgmt	Task Management - Monitor the tasks being executed in the server.
tca	TCA Policy - Parent package for all TCA classes.
tca.TCAManager.property_maxTCAAlarmLimit	TCAManager - property_maxTCAAlarmLimit - TCA preferences can only be modified by a user with an administrator role.
tca.TCAManager.property_maxTCAAlarmResetInterv al	TCAManager - property_maxTCAAlarmResetInterval - TCA preferences can only be modified by a user with an administrator role.
tdmequipment	TDM Equipment - TDM Equipment configuration.
telcoacg	Telco Access Group - Access Groups for Ethernet Ports.
telcoaclfilter	Telco ACL Filter - 7250 SAS and Telco ACL Filters: Standard IP, Extended IP, IGMP, and MAC.
telcoqos	Telco QoS - 7250 SAS and Telco QoS Node Level Policy, QoS MAC Policy for layer2.Bridge, and QoS for Ethernet Ports.
template	Service Template - Deprecated 6.0: use XML API based configuration templates (see class script.XmlApiConfigTemplate).
tod	TOD - Time Of Day Range Policy.
todsuite	TOD Suite - Time Of Day Suite Policy for Egress and Ingress Entries.
topology	CPAM: Topology - All CPAM topology configurations including BGP, IS-IS, OSPF, CPAA, Links, Routers, Areas, Subnets, Checkpoints, and Route Alarms.
topology.Checkpoint.method_autoCreateCheckpoint s	Checkpoint - method_autoCreateCheckpoints - Ability to create checkpoints for protocols within the an IGP admin domain.
topology.IsisCheckpoint	ISIS Checkpoint - Access to snapshots (checkpoints) for a specific ISIS routing domain.
topology.IsisCpSchedulePolicy	ISIS Checkpoint Schedule Policy - Access to configure Checkpoint Schedule Policies for ISIS routing domains.
topology.OspfCheckpoint	OSPF Checkpoint - Access to snapshots (checkpoints) for a specific OSPF area.

(18 of 20)

Package.Class.Method/Property	Description
topology.OspfCpSchedulePolicy	OSPF Checkpoint Schedule Policy - Access to configure Checkpoint Schedule Policies for OSPF areas.
topologysim	CPAM: Simulated Topology - CPAM simulated IGP topology including Links, Routers, Areas, Subnets, and IP Paths.
trapmapper	Trap to Alarm Mapper - Trap to Alarm Mapper.
tunnelmgmt	Tunnel Management - All Tunnel related objects including Hubs, Spokes, Meshes, Chains, Rings, Two Neighbor, Class Forwarding and Rule-based Groups.
udprelay	UDP Relay - UDP Relay configuration and services for layer2.Bridge, DHCP Snooping for VLANs and Ports.
udptunnel	UDP Tunnel - Access to UDP Tunnel.
user	User Preference - SAM Client GUI preferences for Info Tables.
userlog	User Log - SAM Usage and Activity Logs.
vlan	VLAN - Access to this package is for configuring TLS, MVR, Super VLAN, Customer VLAN, SAP and MSAP, Network Interfaces (Uplink Ports) and VLAN configuration for a MST Instance.
vlan.EthernetService	VLAN Ethernet Service - Access to VLAN Ethernet Services.
vlan.L2AccessInterface	VLAN Access Interface - Access to VLAN Access Interfaces.
vlan.Site	VLAN Site - Access to VLAN Sites.
vlan.Vlan	VLAN Service - Access to Virtual LAN (VLAN) Service objects themselves.
vll	VLL - All contained objects are listed. Package access is not currently used.
vll.Endpoint	Endpoint - Access to VLL Endpoints.
vll.L2AccessInterface	L2 Access Interface - Access to VLL L2 Access Interfaces (except Ipipe).
vpls	VPLS - Access to this package is for configuring MLD Snooping, PIM Snooping, DHCP Relay, Multicast CAC Level and LAG Port Down events, and discovered VLAN Elements.
vpls.BL2AccessInterface	VPLS B-L2 Access Interface - Access to VPLS B-L2 Access Interfaces on a VPLS Service.
vpls.BSite	VPLS B-Site - Access to VPLS B-Sites on a VPLS Service.
vpls.Endpoint	VPLS Endpoint - Access to VPLS Endpoints on a VPLS Service.
vpls.IL2AccessInterface	VPLS I-L2 Access Interface - Access to VPLS I-L2 Access Interfaces on a VPLS Service.
vpls.ISite	VPLS I-Site - Access to VPLS I-Sites on a VPLS Service.
vpls.L2AccessInterface	VPLS L2 Access Interface - Access to VPLS L2 Access Interfaces (except I and B) on a VPLS Service.
vpls.L2ManagementInterface	VPLS L2 Management Interface - Access to VPLS L2 Management Interfaces on a VPLS Service.
vpls.Site	VPLS Site - Access to VPLS Sites (except I and B) on a VPLS Service.
vpls.Vpls	VPLS Service - Access to Virtual Private LAN Service (VPLS) Service objects themselves.

(19 of 20)

Package.Class.Method/Property	Description
vprn	VPRN - Access to this package is for configuring VPRN Router Instance Sites, SNMP Community, IPsec Interfaces, Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for VPRN specific SAPs.
vprn.IPMirrorInterface	IP Mirror Interface - Access to VPRN IP Mirror Interfaces.
vprn.L3AccessInterface	VPRN L3 Access Interface - Access to VPRN L3 Access Interfaces.
vprn.Site	VPRN Site - Access to VPRN Sites.
vprn.SubscriberInterface	VPRN Subscriber Interface - Access to VPRN Subscriber Interfaces.
vprn.Vprn	VPRN Service - Access to Virtual Private Routed Network (VPRN) Service objects themselves.
vprn.VprnPing	VPRN Ping - Access to VPRN Ping tests, VPRN Ping test definitions, and VPRN Ping deployed tests.
vprn.VprnTrace	VPRN Trace - Access to VPRN Trace tests, VPRN Trace test definitions, and VPRN Trace deployed tests.
vrrp	VRRP - Virtual Router Redundancy Protocol (VRRP) configuration on rtr.NetworkInterface, IES and VPRN access interfaces, Authentication Keys, Priority Control Policies and Events.
vs	Scheduler Policy - Scheduler Policies.

(20 of 20)

A.3 Permissions of predefined scope of command roles

This section describes the permissions of each default scope of command role. Each permission can have the following access levels to an object package, class, method or property:

- Read-only—provides read access to an object class without the ability to create or delete objects.
- Read/write—provides full access to an object class that includes read, create, update/execute, and delete access.
- Read/update/execute—provides read and update/execute access to an object package or property, but does not provide delete access.
- Update/execute—provides update/execute access on class methods, and is typically combined with read access on the parent object package.
- No access.

Note — This appendix does not list permissions with read-only access. Permissions that are not listed for a predefined scope of command role have an access level of read-only.

Table A-4 lists the default scope of command roles and provides links to their respective permissions tables.

Table A-4 Scope of command roles

Role	Link
Base Read-only	Table A-5
Administrator	Table A-6
User Management	Table A-7
Network Element Equipment Manager	Table A-8
Service Management	Table A-9
Subscriber Management	Table A-10
QoS/ACL Policy Management	Table A-11
Policy Management (except QoS/ACL)	Table A-12
Routing Management	Table A-13
Tunnel Management	Table A-14
SAM Management and Operations	Table A-15
Network Element Software Management	Table A-16
Fault Management	Table A-17
Service Test Management	Table A-18
Script Management	Table A-19
Script Execution	Table A-20
Mirror Service Management	Table A-21
OSS Management	Table A-22
Telnet/SSH Management	Table A-23
CPAM Management	Table A-24
CPAM OSS PCA	Table A-25
CPAM Topology Simulator	Table A-26
Root Cause Analysis (RCA) Object Verification	Table A-27
Lawful Intercept Management	Table A-28
Template Script Management	Table A-29
Service Template Script Execution	Table A-30
Tunnel Template Script Execution	Table A-31
Application Assurance (AA) Management	Table A-32
Format and Range Policy Management	Table A-33
Work Order Activation	Table A-34
Configuration Snapshot Export	Table A-35
Create and Delete Access	Table A-36
Configuration Management which causes node reset	Table A-37
EPC Operator	Table A-38
eNodeB NEM Operator	Table A-39

Table A-5 Base Read-only

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access

(1 of 3)

Package.Class.Method/Property	Access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access

(2 of 3)

Package.Class.Method/Property	Access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-6 Administrator

Package.Class.Method/Property	Access
aapolicy	Read/write
accessuplink	Read/write
accounting	Read/write
aclfilter	Read/write
activation	Read/write
activation.Session	Read/write
activation.Snapshot	Read/write
activation.SnapshotEntity	Read/write
activation.WebDAVSharedData	Read/write
activation.WorkOrder	Read/write
aengr	Read/write
aingr	Read/write
ancp	Read/write
ancp.AncpLoopback	Read/write
antispoof	Read/write
aosqos	Read/write
aossas	Read/write
aossas.CPETestGroupHead	Read/write
aossas.CPETestHead	Read/write
apipe	Read/write
apipe.Apipe	Read/write
apipe.Site	Read/write
aps	Read/write
arp	Read/write
atm	Read/write
atm.AtmPing	Read/write
atmpolicy	Read/write

(1 of 14)

Package.Class.Method/Property	Access
audit	Read/write
autoconfig	Read/write
autoconfig.AutoConfigScriptManager.method_configure	Update/execute
autoconfig.AutoConfigScriptManager.method_copyContents	Update/execute
bfd	Read/write
bgp	Read/write
bgp.Site	Read/write
bulk	Read/write
bulk.BulkChange	Read/write
bulk.BulkManager.method_execute	Update/execute
bulk.BulkManager.method_generateBatches	Update/execute
bundle	Read/write
cac	Read/write
ccag	Read/write
cflowd	Read/write
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
circem	Read/write
clear	Read/write
cli	Read/write
cli.SSH	Read/write
cli.Telnet	Read/write
connprof	Read/write
cpipe	Read/write
cpipe.Cpipe	Read/write
cpipe.Site	Read/write
crdtctrl	Read/write
customproperties	Read/write
db	Read/write
db.DatabaseManager.method_backup	Update/execute
db.DatabaseManager.method_reinstantiateStandby	Update/execute
db.DatabaseManager.method_switchover	Update/execute
dhcp	Read/write
diameter	Read/write
epipe	Read/write
epipe.Epipe	Read/write
epipe.PbbMacName	Read/write

(2 of 14)

Package.Class.Method/Property	Access
epipe.Site	Read/write
equipment	Read/write
ethernetequipment	Read/write
ethernetoam	Read/write
ethernetoam.CcTest	Read/write
ethernetoam.CcmTest	Read/write
ethernetoam.CfmEthTest	Read/write
ethernetoam.CfmLinkTrace	Read/write
ethernetoam.CfmLoopback	Read/write
ethernetoam.CfmOneWayDelayTest	Read/write
ethernetoam.CfmOneWaySlm	Read/write
ethernetoam.CfmSingleEndedLossTest	Read/write
ethernetoam.CfmTwoWayDelayTest	Read/write
ethernetoam.CfmTwoWaySlm	Read/write
ethernetservice	Read/write
ethernettunnel	Read/write
ethring	Read/write
fabricqos	Read/write
file	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	Update/execute
fm.FaultManager	Read/write
fm.FaultManager.method_editNote	Update/execute
fm.GlobalPolicy	Read/write
fm.SpecificPolicy	Read/write
fpipe	Read/write
fpipe.Fpipe	Read/write
fpipe.Site	Read/write
fr	Read/write
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
genericne	Read/write
gsmp	Read/write
hip.EMServer	Read/write
hip.EMSystem	Read/write
hpipe	No access

(3 of 14)

Package.Class.Method/Property	Access
hpipe.Hpipe	Read/write
hpipe.Site	Read/write
icmp.DnsPing	Read/write
icmp.IcmpPing	Read/write
icmp.IcmpTrace	Read/write
ies	Read/write
ies.Ies	Read/write
ies.L3AccessInterface	Read/write
ies.Site	Read/write
ies.SubscriberInterface	Read/write
igh	Read/write
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	Read/write
impact.PartialReset	Read/write
ipipe	Read/write
ipipe.Ipipe	Read/write
ipipe.L2AccessInterface	Read/write
ipipe.Site	Read/write
ipsec	Read/write
isa	Read/write
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write
isis	Read/write
l2fib	Read/write
l2fwd	Read/write
l2tp	Read/write
l3fwd	Read/write
lag	Read/write
layer2	Read/write
ldp	Read/write
lldp	Read/write
localuserdb	Read/write
log	Read/write
log.LogToFileManager.property_retention	Read/update/execute
log.LogToFileManager.property_rollover	Read/update/execute
lps	Read/write

(4 of 14)

Package.Class.Method/Property	Access
lte	Read/write
lte.CallTraceDirectory	Read/write
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write
lte.DiameterProfile	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	Update/execute
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write
lte.EPSPathSegment	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.IpPool	Read/write
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.MobileNodeRegion	Read/write
lte.PDNGateway	Read/write
lte.PdnApn	Read/write
lte.PdnGxReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write
lte.QciPolicyEntry	Read/write
lte.S11ReferencePoint	Read/write

(5 of 14)

Package.Class.Method/Property	Access
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwChargingProfile	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lte.SubscAndEquipmentTraces	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lte.TrustedPeerListPolicy	Read/write
lteanr	Read/write
lteggsn	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write
lteggsn.SgwGaReferencePoint	Read/write
ltemme	Read/write
ltemme.MmeInstance.method_abortMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_interMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_intraMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_lockMmeAggregateService	Update/execute
ltemme.MmeInstance.method_unlockMmeAggregateService	Update/execute
lteperf	Read/write
ltepmip	Read/write
ltepmip.Pmipv6Profile	Read/write
ltepmip.S2aReferencePoint	Read/write
ltepool	Read/write
ltepool.MmeInstanceBinding	Read/write
ltepool.TaBinding	Read/write
lteradius	Read/write
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
lteradius.RadiusProfile	Read/write
ltes1mme	Read/write
ltesecurity	Read/write

(6 of 14)

Package.Class.Method/Property	Access
lteservice	Read/write
ltethreshold	Read/write
lteuserstats	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write
lteuserstats.UserStatsUserSgw	Read/write
mediation	Read/write
mirror	Read/write
mirror.Endpoint	Read/write
mirror.Mirror	Read/write
mirror.Site	Read/write
mld	Read/write
mmepolicy	No access
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
monitor	Read/write
monpath	Read/write
mpls	Read/write
mpls.LdpTreeTrace	Read/write
mpls.LspPing	Read/write
mpls.LspTrace	Read/write
mpls.P2MPLspPing	Read/write
mpls.P2MPLspTrace	Read/write
mpr	Read/write
mpr.Al2AccessInterface	Read/write
mpr.Apipe	Read/write
mpr.Asite	Read/write
mpr.Cpipe	Read/write
mpr.El2AccessInterface	Read/write
mpr.Epipe	Read/write
mpr.Esite	Read/write
mpr.L2AccessInterface	Read/write
mpr.Site	Read/write
msappolicy	Read/write
msdp	Read/write
multicast	Read/write

(7 of 14)

Package.Class.Method/Property	Access
multicast.CustomerVlanTag	Read/write
multicast.MfibPing	Read/write
multicast.Mrinfo	Read/write
multicast.Mtrace	Read/write
multicastmgr	Read/write
multichassis	Read/write
mvpls	Read/write
mvpls.BL2AccessInterface	Read/write
mvpls.BSite	Read/write
mvpls.IL2AccessInterface	Read/write
mvpls.ISite	Read/write
mvpls.L2AccessInterface	Read/write
mvpls.Mvpls	Read/write
mvpls.Site	Read/write
mvrp	Read/write
nat	Read/write
netca	Read/write
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	Update/execute
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
niegr	Read/write
nodelog	Read/write
nqueue	Read/write
ntp	Read/write
optical	Read/write
optical.DiverseService	Read/write
optical.SubRateService	Read/write
optical.TransportService	Read/write
optical.YCableService	Read/write
opticsperf	Read/write

(8 of 14)

Package.Class.Method/Property	Access
ospf	Read/write
ospf.Site	Read/write
oss	No access
pae802_1x	Read/write
pim	Read/write
pim.Site	Read/write
policing	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
portscheduler	Read/write
ppp	Read/write
pppoe	Read/write
propertyrules	Read/write
ptp	Read/write
qgroup	Read/write
qosprofile	Read/write
radioequipment	Read/write
radiusaccounting	Read/write
ranlicense	Read/write
ranradiom	Read/write
rca	Read/write
rca.RcaManager.method_fixProblem	Update/execute
rca.RcaManager.method_preFixProblem	Update/execute
resiliency	Read/write
resources	Read/write
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.SubMcastCacPolicy	Read/write
rip	Read/write
rip.Site	Read/write
rmon	Read/write
rp	Read/write

(9 of 14)

Package.Class.Method/Property	Access
rsvp	Read/write
rtr	Read/write
rules	Read/write
sas	Read/write
sas.TestManager.property_sasRetention	Read/update/execute
sas.TestManager.property_sasRollover	Read/update/execute
sasqos	Read/write
sasqos.QosPool	Read/write
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.Bundle	Read/write
script.ControlScript	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.LargeTextTargetParameter	Read/write
script.Result	Read/write
script.Script	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	Update/execute
script.ScriptManager.method_copyContents	Update/execute
script.ScriptManager.method_exportBundle	Update/execute
script.ScriptManager.method_importBundle	Update/execute
script.ScriptManager.method_importBundleSimulation	Update/execute
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.TemplateBinding	Read/write
script.Version	Read/write
script.XmlApiConfigTemplate	Read/write
script.XmlApiConfigTemplate.method_execute	Update/execute

(10 of 14)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
script.XmlApiScript	Read/write
script.XmlApiVersion	Read/write
security	Read/write
security.CpamLicense	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	Update/execute
security.CpamLicenseScenario	Read/write
security.MediationPolicy	Read/write
security.MessagingConnection	Read/write
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	Read/write
security.ScopeOfCommandRole	Read/write
security.Span	Read/write
security.SpanObjectBinding	Read/write
security.SpanOfControlProfile	Read/write
security.User	Read/write
security.UserGroup	Read/write
selfconfig	Read/write
server	Read/write
service	Read/write
service.CpePing	Read/write
service.GneAccessInterface	Read/write
service.GneSite	Read/write
service.MacPing	Read/write
service.MacPopulate	Read/write
service.MacPurge	Read/write
service.MacTrace	Read/write
service.MefMacPing	Read/write
service.RedundantInterface	Read/write
service.Service.method_create	Update/execute
service.Service.method_highPriorityServiceDelete	Update/execute
service.Service.property_svcPriority	Read/update/execute
service.ServiceManager.property_alarmAggregationCompositeService	Read/update/execute
service.ServiceManager.property_autoDiscoverCompositeSvc	Read/update/execute

(11 of 14)

Package.Class.Method/Property	Access
service.ServiceManager.property_enableCac	Read/update/execute
service.ServiceManager.property_maxNumberOfMoveSites	Read/update/execute
service.ServiceManager.property_multiSegmentTunnelSelection	Read/update/execute
service.ServiceManager.property_propagateServiceNameToSites	Read/update/execute
service.ServiceManager.property_removeEmptyService	Read/update/execute
service.ServiceManager.property_supVprnSnmpCommunityStringMsg	Read/update/execute
service.ServiceManager.property_svcPriority	Read/update/execute
service.ServiceMemberAuditPolicyEntry	Read/write
service.SitePing	Read/write
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	Update/execute
shg	Read/write
simulator	Read/write
simulator.SimSession	Read/write
sitesec	Read/write
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
slaprofile	Read/write
slope	Read/write
slope.QosPool	Read/write
snmp	Read/write
snmp.EventNotificationPolicy	Read/write
snmp.PollerManager	Read/write
snmp.PollerManager.method_resync	Update/execute
sonet	Read/write
sonetequipment	Read/write
spanrules	Read/write
squeue	Read/write
srmrmtauth	Read/write
srrp	Read/write
statistics	Read/write
subscr	Read/write
subscr.Site	Read/write
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write

(12 of 14)

Package.Class.Method/Property	Access
sup	Read/write
svq	Read/write
svr	Read/write
svt	Read/write
svt.MeshSdpBinding	Read/write
svt.MirrorSdpBinding	Read/write
svt.MtuPing	Read/write
svt.SpokeSdpBinding	Read/write
svt.Tunnel	Read/write
svt.TunnelPing	Read/write
svt.VccvPing	Read/write
svt.VccvTrace	Read/write
sw	Read/write
sw.BackupRestoreManager.method_backup	Update/execute
sw.BackupRestoreManager.method_restore	Update/execute
swran	Read/write
tca	Read/write
tca.TCAManager.property_maxTCAAlarmLimit	Read/update/execute
tca.TCAManager.property_maxTCAAlarmResetInterval	Read/update/execute
tdmequipment	Read/write
telcoacg	Read/write
telcoaclfilter	Read/write
telcoqos	Read/write
template	Read/write
tod	Read/write
todsuite	Read/write
topology	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	Update/execute
topology.IsisCheckpoint	Read/write
topology.IsisCpSchedulePolicy	Read/write
topology.OspfCheckpoint	Read/write
topology.OspfCpSchedulePolicy	Read/write
topologysim	Read/write
trapmapper	Read/write
tunnelmgmt	Read/write
udprelay	Read/write
udptunnel	Read/write

(13 of 14)

Package.Class.Method/Property	Access
user	Read/write
userlog	Read/write
vlan	Read/write
vlan.EthernetService	Read/write
vlan.L2AccessInterface	Read/write
vlan.Site	Read/write
vlan.Vlan	Read/write
vll	Read/write
vll.Endpoint	Read/write
vll.L2AccessInterface	Read/write
vpls	Read/write
vpls.BL2AccessInterface	Read/write
vpls.BSite	Read/write
vpls.Endpoint	Read/write
vpls.IL2AccessInterface	Read/write
vpls.ISite	Read/write
vpls.L2AccessInterface	Read/write
vpls.L2ManagementInterface	Read/write
vpls.Site	Read/write
vpls.Vpls	Read/write
vprn	Read/write
vprn.IPMirrorInterface	Read/write
vprn.L3AccessInterface	Read/write
vprn.Site	Read/write
vprn.SubscriberInterface	Read/write
vprn.Vprn	Read/write
vprn.VprnPing	Read/write
vprn.VprnTrace	Read/write
vrrp	Read/write
vs	Read/write

(14 of 14)

Table A-7 User management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access

(1 of 4)

Package.Class.Method/Property	Access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access

(2 of 4)

Package.Class.Method/Property	Access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security	Read/update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access

(3 of 4)

Package.Class.Method/Property	Access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-8 Network Element Equipment Manager

Package.Class.Method/Property	Access
aapolicy	Read/write
accessuplink	Read/write
activation.WebDAVSharedData	No access
aps	Read/write
atm	Read/write
audit	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
bundle	Read/write
cac	Read/write
ccag	Read/write
cflowd	Read/write
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
circem	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
equipment	Read/write
ethernetequipment	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
fr	Read/write
generic	Read/write

(1 of 4)

Package.Class.Method/Property	Access
generic.GenericObject.method_collectData	No access
hpipe	No access
igh	Read/write
impact.FullReset	No access
impact.PartialReset	No access
ipsec	Read/write
isa	Read/write
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write
l2fib	Read/write
lag	Read/write
lldp	Read/write
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.SubscAndEquipmentTraces	Read/write
lteanr	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme	Read/write
ltemme.MmeInstance.method_abortMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_interMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_intraMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_lockMmeAggregateService	Update/execute
ltemme.MmeInstance.method_unlockMmeAggregateService	Update/execute
ltepool	Read/write
ltepool.MmeInstanceBinding	Read/write
ltepool.TaBinding	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpr	Read/write
multichassis	Read/write
nat	Read/write
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
ntp	Read/write
optical	Read/write
oss	No access
pae802_1x	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
ppp	Read/write
ptp	Read/write
radioequipment	Read/write
ranlicense	Read/write
ranradiom	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
sasqos.QosPool	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access

(3 of 4)

Package.Class.Method/Property	Access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
selfconfig	Read/write
service	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
slope.QosPool	Read/write
snmp.PollerManager.method_resync	Update/execute
sonet	Read/write
sonetequipment	Read/write
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
tdmequipment	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-9 Service Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
ancp	Read/write
antispoof	Read/write
apipe	Read/write
apipe.Apipe	Read/write
apipe.Site	Read/write

(1 of 6)

Package.Class.Method/Property	Access
arp	Read/write
atm	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bfd	Read/write
bgp.Site	Read/write
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cac	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
cpipe	Read/write
cpipe.Cpipe	Read/write
cpipe.Site	Read/write
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
dhcp	Read/write
epipe	Read/write
epipe.Epipe	Read/write
epipe.PbbMacName	Read/write
epipe.Site	Read/write
ethernettunnel	Read/write
ethring	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
fpipe	Read/write
fpipe.Fpipe	Read/write
fpipe.Site	Read/write
generic	Read/write
generic.GenericObject.method_collectData	No access
gsmp	Read/write
hpipe	No access
hpipe.Hpipe	Read/write
hpipe.Site	Read/write

(2 of 6)

Package.Class.Method/Property	Access
ies	Read/write
ies.Ies	Read/write
ies.L3AccessInterface	Read/write
ies.Site	Read/write
ies.SubscriberInterface	Read/write
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	No access
impact.PartialReset	No access
ipipe	Read/write
ipipe.Ipipe	Read/write
ipipe.L2AccessInterface	Read/write
ipipe.Site	Read/write
ipsec	Read/write
l2fib	Read/write
l2fwd	Read/write
l2tp	Read/write
l3fwd	Read/write
layer2	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Endpoint	Read/write
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpr	Read/write
mpr.Al2AccessInterface	Read/write
mpr.Apipe	Read/write
mpr.Asite	Read/write
mpr.Cpipe	Read/write

(3 of 6)

Package.Class.Method/Property	Access
mpr.El2AccessInterface	Read/write
mpr.Epipe	Read/write
mpr.Esite	Read/write
mpr.L2AccessInterface	Read/write
mpr.Site	Read/write
mvpls	Read/write
mvpls.BL2AccessInterface	Read/write
mvpls.BSite	Read/write
mvpls.IL2AccessInterface	Read/write
mvpls.ISite	Read/write
mvpls.L2AccessInterface	Read/write
mvpls.Mvpls	Read/write
mvpls.Site	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
optical	Read/write
optical.DiverseService	Read/write
optical.SubRateService	Read/write
optical.TransportService	Read/write
optical.YCableService	Read/write
ospf	Read/write
ospf.Site	Read/write
oss	No access
pim	Read/write
pim.Site	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
rip	Read/write
rip.Site	Read/write
rtr	Read/write

(4 of 6)

Package.Class.Method/Property	Access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service	Read/write
service.GneAccessInterface	Read/write
service.GneSite	Read/write
service.RedundantInterface	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	No access
shg	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
srrp	Read/write
svt	Read/write
svt.MeshSdpBinding	Read/write
svt.MirrorSdpBinding	No access

(5 of 6)

Package.Class.Method/Property	Access
svt.SpokeSdpBinding	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
template	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vlan	Read/write
vlan.EthernetService	Read/write
vlan.L2AccessInterface	Read/write
vlan.Site	Read/write
vlan.Vlan	Read/write
vll	Read/write
vll.Endpoint	Read/write
vll.L2AccessInterface	Read/write
vpls	Read/write
vpls.BL2AccessInterface	Read/write
vpls.BSite	Read/write
vpls.Endpoint	Read/write
vpls.IL2AccessInterface	Read/write
vpls.ISite	Read/write
vpls.L2AccessInterface	Read/write
vpls.L2ManagementInterface	Read/write
vpls.Site	Read/write
vpls.Vpls	Read/write
vprn	Read/write
vprn.IPMirrorInterface	No access
vprn.L3AccessInterface	Read/write
vprn.Site	Read/write
vprn.SubscriberInterface	Read/write
vprn.Vprn	Read/write
vrrp	Read/write

(6 of 6)

Table A-10 Subscriber Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
ancp	Read/write
arp	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
connprof	Read/write
crdtctrl	Read/write
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
diameter	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write
impact.FullReset	No access
impact.PartialReset	No access
l2tp	Read/write
localuserdb	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
monitor	Read/write
msappolicy	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
policy.PolicySyncGroupManager	Read/write
pppoe	Read/write
radiusaccounting	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.SubMcastCacPolicy	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
slaprofile	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
subscr	Read/write
subscr.Site	Read/write
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
telcoacg	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-11 QoS/ACL Policy Management

Package.Class.Method/Property	Access
aclfilter	Read/write
activation.WebDAVSharedData	No access
aengr	Read/write
aingr	Read/write
aosqos	Read/write
aossas	Read/write
atmpolicy	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
ethernetservice	Read/write
fabricqos	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
layer2	Read/write
lte	Read/update/execute
lte.DiameterProfile	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.TrustedPeerListPolicy	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
lteradius.RadiusProfile	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpr	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
niegr	Read/write
nqueue	Read/write
oss	No access
policing	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
portscheduler	Read/write
qgroup	Read/write
qosprofile	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
sasqos	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access

(2 of 3)

Package.Class.Method/Property	Access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
slope	Read/write
snmp.PollerManager.method_resync	No access
squeue	Read/write
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
telcoaclfilter	Read/write
telcoqos	Read/write
todsuite	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access
vs	Read/write

(3 of 3)

Table A-12 Policy Management (except QoS/ACL)

Package.Class.Method/Property	Access
accounting	Read/write
activation.WebDAVSharedData	No access
ancp	Read/write
aossas	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
connprof	Read/write
crdtctrl	Read/write
db	Read/write
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
diameter	Read/write
ethernetoam	Read/write
file	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write
impact.FullReset	No access
impact.PartialReset	No access
l2fwd	Read/write
lte	Read/update/execute
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write

(1 of 4)

Package.Class.Method/Property	Access
lte.ENBEquipment.method_launchNEM	No access
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write
lte.QciPolicyEntry	Read/write
lte.SgwChargingProfile	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip.Pmipv6Profile	Read/write
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
mpr	Read/write
msappolicy	Read/write
multicast	Read/write
netca	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
nodelog	Read/write

(2 of 4)

Package.Class.Method/Property	Access
oss	No access
pae802_1x	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
pppoe	Read/write
radiusaccounting	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.SubMcastCacPolicy	Read/write
rp	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access

(3 of 4)

Package.Class.Method/Property	Access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
slaprofile	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
tod	Read/write
todsuite	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access
vrrp	Read/write

(4 of 4)

Table A-13 Routing Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bfd	Read/write
bgp	Read/write
bgp.Site	Read/write
bulk.BulkManager.method_execute	No access

(1 of 5)

Package.Class.Method/Property	Access
bulk.BulkManager.method_generateBatches	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	No access
impact.PartialReset	No access
isis	Read/write
l2fib	Read/write
l2tp	Read/write
l3fwd	Read/write
lag	Read/write
layer2	Read/write
ldp	Read/write
lte	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.IpPool	Read/write

(2 of 5)

Package.Class.Method/Property	Access
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.PDNGateway	Read/write
lte.PdnApn	Read/write
lte.PdnGxReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write
lte.S11ReferencePoint	Read/write
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lteggsn	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write
lteggsn.SgwGaReferencePoint	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip.S2aReferencePoint	Read/write
lteradius	Read/write
ltethreshold	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mld	Read/write
mmepolicy	No access
mpls	Read/write

(3 of 5)

Package.Class.Method/Property	Access
mpr	Read/write
msdp	Read/write
multicast	Read/write
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
optical	Read/write
ospf	Read/write
ospf.Site	Read/write
oss	No access
pim	Read/write
pim.Site	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rip	Read/write
rip.Site	Read/write
rp	Read/write
rsvp	Read/write
rtr	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access

(4 of 5)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
udprelay	Read/write
user	Read/write
userlog	No access
vpls	Read/write
vprn.IPMirrorInterface	No access
vrrp	Read/write

(5 of 5)

Table A-14 Tunnel Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access

(1 of 4)

Package.Class.Method/Property	Access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
ipsec	Read/write
ldp	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteanr	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
lteperf	Read/write
ltesecurity	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
mpr	Read/write

(2 of 4)

Package.Class.Method/Property	Access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
opticsperf	Read/write
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rsvp	Read/write
rtr	Read/write
rules	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access

(3 of 4)

Package.Class.Method/Property	Access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt	Read/write
svt.MirrorSdpBinding	No access
svt.Tunnel	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
tunnelmgmt	Read/write
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-15 SAM Management and Operations

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db	Read/write
db.DatabaseManager.method_backup	Update/execute
db.DatabaseManager.method_reinstantiateStandby	Update/execute
db.DatabaseManager.method_switchover	Update/execute

(1 of 5)

Package.Class.Method/Property	Access
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
hip.EMServer	Read/write
hip.EMSystem	Read/write
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
log	Read/write
lps	Read/write
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathSegment	Read/write
lte.MobileNodeRegion	Read/write
lteanr	Read/write
lteggsn	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
lteperf	Read/write
ltepmip	Read/write
lteradius	Read/write
ltesecurity	Read/write
lteservice	Read/write
lteuserstats	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write

(2 of 5)

Package.Class.Method/Property	Access
lteuserstats.UserStatsUserSgw	Read/write
mediation	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
multicast	Read/write
nat	Read/write
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
opticsperf	Read/write
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
ranlicense	Read/write
ranradiom	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access

(3 of 5)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security	Read/update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	Read/write
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.Span	Read/write
security.SpanObjectBinding	Read/write
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
selfconfig	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
snmp	Read/write
snmp.PollerManager	Read/write
snmp.PollerManager.method_resync	Update/execute
spanrules	Read/write
srmrmtauth	No access
statistics	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
tca	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access

(4 of 5)

Package.Class.Method/Property	Access
user	Read/write
userlog	Read/write
vprn.IPMirrorInterface	No access

(5 of 5)

Table A-16 Network Element Software Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	Read/write
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mediation	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology.method_move	No access
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access

(2 of 3)

Package.Class.Method/Property	Access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	Update/execute
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw	Read/write
sw.BackupRestoreManager.method_backup	Update/execute
sw.BackupRestoreManager.method_restore	Update/execute
swran	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-17 Fault Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access

(1 of 3)

Package.Class.Method/Property	Access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	Update/execute
fm.FaultManager	Read/write
fm.FaultManager.method_editNote	Update/execute
fm.GlobalPolicy	Read/write
fm.SpecificPolicy	Read/write
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rmon	Read/write

(2 of 3)

Package.Class.Method/Property	Access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-18 Service Test Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
ancp.AncpLoopback	Read/write
aosqos	Read/write
aossas	Read/write
aossas.CPETestGroupHead	Read/write
aossas.CPETestHead	Read/write
atm.AtmPing	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
ethernetequipment	Read/write
ethernetoam	Read/write
ethernetoam.CcTest	Read/write
ethernetoam.CcmTest	Read/write
ethernetoam.CfmEthTest	Read/write
ethernetoam.CfmLinkTrace	Read/write
ethernetoam.CfmLoopback	Read/write
ethernetoam.CfmOneWayDelayTest	Read/write
ethernetoam.CfmOneWaySlm	Read/write
ethernetoam.CfmSingleEndedLossTest	Read/write
ethernetoam.CfmTwoWayDelayTest	Read/write
ethernetoam.CfmTwoWaySlm	Read/write
ethernettunnel	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access

(1 of 4)

Package.Class.Method/Property	Access
hpipe	No access
icmp.DnsPing	Read/write
icmp.IcmpPing	Read/write
icmp.IcmpTrace	Read/write
impact.FullReset	No access
impact.PartialReset	No access
ldp	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
mpls.LdpTreeTrace	Read/write
mpls.LspPing	Read/write
mpls.LspTrace	Read/write
mpls.P2MPLspPing	Read/write
mpls.P2MPLspTrace	Read/write
multicast.MfibPing	Read/write
multicast.Mrinfo	Read/write
multicast.Mtrace	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access

(2 of 4)

Package.Class.Method/Property	Access
rca.RcaManager.method_preFixProblem	No access
resources	No access
sas	Read/write
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.CpePing	Read/write
service.MacPing	Read/write
service.MacPopulate	Read/write
service.MacPurge	Read/write
service.MacTrace	Read/write
service.MefMacPing	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.SitePing	Read/write
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access

(3 of 4)

Package.Class.Method/Property	Access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
svt.MtuPing	Read/write
svt.TunnelPing	Read/write
svt.VccvPing	Read/write
svt.VccvTrace	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access
vprn.VprnPing	Read/write
vprn.VprnTrace	Read/write

(4 of 4)

Table A-19 Script Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig	Read/write
autoconfig.AutoConfigScriptManager.method_configure	Update/execute
autoconfig.AutoConfigScriptManager.method_copyContents	Update/execute
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access

(1 of 4)

Package.Class.Method/Property	Access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.Bundle	Read/write
script.ControlScript	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.LargeTextTargetParameter	Read/write
script.Result	Read/write

(2 of 4)

Package.Class.Method/Property	Access
script.Script	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	Update/execute
script.ScriptManager.method_copyContents	Update/execute
script.ScriptManager.method_exportBundle	Update/execute
script.ScriptManager.method_importBundle	Update/execute
script.ScriptManager.method_importBundleSimulation	Update/execute
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.Version	Read/write
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
script.XmlApiScript	Read/write
script.XmlApiVersion	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access

(3 of 4)

Package.Class.Method/Property	Access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-20 Script Execution

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.LargeTextTargetParameter	Read/write
script.Result	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-21 Mirror Service Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access

(1 of 4)

Package.Class.Method/Property	Access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
ethernetequipment	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	Read/write
mirror.Mirror	Read/write
mirror.Site	Read/write
mmepolicy	No access
mpls	Read/write
mpr	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access

(2 of 4)

Package.Class.Method/Property	Access
rca.RcaManager.method_preFixProblem	No access
resources	No access
sas	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service	Read/write
service.GneAccessInterface	Read/write
service.GneSite	Read/write
service.Service.method_create	Update/execute
service.Service.method_highPriorityServiceDelete	Update/execute
service.SitePing	Read/write
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	Update/execute
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
subscr.Site	Read/write
svt	Read/write

(3 of 4)

Package.Class.Method/Property	Access
svt.MirrorSdpBinding	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
template	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	Read/write

(4 of 4)

Table A-22 OSS Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access

(2 of 3)

Package.Class.Method/Property	Access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-23 Telnet/SSH Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	Read/write
cli.SSH	Read/write
cli.Telnet	Read/write
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write

(1 of 3)

Package.Class.Method/Property	Access
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-24 CPAM Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access

(1 of 4)

Package.Class.Method/Property	Access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	Update/execute
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access

(2 of 4)

Package.Class.Method/Property	Access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	Update/execute
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	Update/execute
topology.IsisCheckpoint	Read/write
topology.IsisCpSchedulePolicy	Read/write
topology.OspfCheckpoint	Read/write
topology.OspfCpSchedulePolicy	Read/write
user	Read/write
userlog	No access

(3 of 4)

Package.Class.Method/Property	Access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-25 CPAM OSS PCA

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access

(1 of 3)

Package.Class.Method/Property	Access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access

(2 of 3)

Package.Class.Method/Property	Access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology	Read/write
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-26 CPAM Topology Simulator

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access

(1 of 3)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access

(2 of 3)

Package.Class.Method/Property	Access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
simulator	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
topologysim	Read/write
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-27 Root Cause Analysis (RCA) Object Verification

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write

(1 of 3)

Package.Class.Method/Property	Access
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access

(2 of 3)

Package.Class.Method/Property	Access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.ServiceMemberAuditPolicyEntry	Read/write
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-28 Lawful Intercept Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access

(1 of 4)

Package.Class.Method/Property	Access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	Read/write
lteli.InterceptionTarget	Read/write
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror.Mirror	Read/write
mirror.Site	Read/write
mirrorli	Read/write
mmepolicy	No access
netw	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	No access
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access

(3 of 4)

Package.Class.Method/Property	Access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
snmp.PollerManager	Read/write
snmp.PollerManager.method_resync	Update/execute
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-29 Template Script Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access

(1 of 3)

Package.Class.Method/Property	Access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Bundle	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	Update/execute

(2 of 3)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundle	Update/execute
script.ScriptManager.method_importBundleSimulation	Update/execute
script.TemplateBinding	Read/write
script.XmlApiConfigTemplate	Read/write
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
script.XmlApiVersion	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-30 Service Template Script Execution

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access

(1 of 4)

Package.Class.Method/Property	Access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access

(2 of 4)

Package.Class.Method/Property	Access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write

(3 of 4)

Package.Class.Method/Property	Access
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-31 Tunnel Template Script Execution

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access

(1 of 3)

Package.Class.Method/Property	Access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access

(2 of 3)

Package.Class.Method/Property	Access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-32 Application Assurance (AA) Management

Package.Class.Method/Property	Access
aapolicy	Read/write
accounting	Read/write
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
file	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access

(1 of 3)

Package.Class.Method/Property	Access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-33 Format and Range Policy Management

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access

(1 of 3)

Package.Class.Method/Property	Access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
propertyrules	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access

(2 of 3)

Package.Class.Method/Property	Access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
spanrules	Read/write
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-34 Work Order Activation

Package.Class.Method/Property	Access
activation	Read/write
activation.Session	Read/write
activation.WebDAVSharedData	Read/write
activation.WorkOrder	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	Read/write
impact.PartialReset	Read/write
lte	Read/update/execute
lte.ENBEquipment.method_launchNEM	No access
lte.SubscAndEquipmentTraces	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access

(1 of 3)

Package.Class.Method/Property	Access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access

(2 of 3)

Package.Class.Method/Property	Access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-35 Configuration Snapshot Export

Package.Class.Method/Property	Access
activation.Snapshot	Read/write
activation.SnapshotEntity	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access

(1 of 3)

Package.Class.Method/Property	Access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access

(2 of 3)

Package.Class.Method/Property	Access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-36 Create and Delete Access

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access

(1 of 3)

Package.Class.Method/Property	Access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access

(2 of 3)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-37 Configuration Management which causes node reset

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access

(1 of 3)

Package.Class.Method/Property	Access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	Read/write
impact.PartialReset	Read/write
lte.ENBEquipment.method_launchNEM	No access
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access

(2 of 3)

Package.Class.Method/Property	Access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Table A-38 EPC Operator

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write
lte	Read/update/execute
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write
lte.DiameterProfile	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write

(1 of 4)

Package.Class.Method/Property	Access
lte.EPSPathSegment	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.IpPool	Read/write
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.MobileNodeRegion	Read/write
lte.PDNGateway	Read/write
lte.PdnApn	Read/write
lte.PdnGxReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write
lte.QciPolicyEntry	Read/write
lte.S11ReferencePoint	Read/write
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwChargingProfile	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lte.TrustedPeerListPolicy	Read/write
lteggsn	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write

(2 of 4)

Package.Class.Method/Property	Access
lteggsn.SgwGaReferencePoint	Read/write
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip.S2aReferencePoint	Read/write
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
lteradius.RadiusProfile	Read/write
ltethreshold	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write
lteuserstats.UserStatsUserSgw	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access

(3 of 4)

Package.Class.Method/Property	Access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
topology.Checkpoint.method_autoCreateCheckpoints	No access
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(4 of 4)

Table A-39 eNodeB NEM Operator

Package.Class.Method/Property	Access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_switchover	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	Update/execute
lteli.DFPeer	No access
lteli.InterceptionTarget	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access

(1 of 3)

Package.Class.Method/Property	Access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access

(2 of 3)

Package.Class.Method/Property	Access
topology.Checkpoint.method_autoCreateCheckpoints	No access
udptunnel	Read/write
user	Read/write
userlog	No access
vprn.IPMirrorInterface	No access

(3 of 3)

Customer documentation and product support

Customer documentation

http://www.alcatel-lucent.com/myaccess

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 06495 AAAG TQZZA Edition 01